Mutually Unbiased Product Bases

Daniel McNulty

PhD

2013

Mutually Unbiased Product Bases

Daniel McNulty

PhD

University of York

Mathematics

April 2013

Abstract

A pair of orthonormal bases are mutually unbiased (MU) if the inner products across all their elements have equal magnitude. In quantum mechanics, these bases represent observables that are complementary, i.e. a measurement of one observable implies maximal uncertainty about the possible outcome of a subsequent measurement of a second observable. MU bases have attracted interest in recent years because their properties seem to depend dramatically on the dimension d of the quantum system in hand. If the dimension is given by a prime or prime-power, the state space is known to accommodate a *complete* set of $d+1$ MU bases. However, for "composite" dimensions, such as $d = 6, 10, 12, \ldots$, complete sets seem to be absent and it is not understood why. In this thesis we carry out a comprehensive study of MU *product* bases in dimension six. In particular, we construct all MU bases in dimension six consisting of product states only. The exhaustive classification leads to several non-existence results. We also present a new construction of complex Hadamard matrices of composite order, which is a consequence of our work on MU product bases. Based on this construction we obtain several new isolated Hadamard matrices of Butson-type.

Contents

Acknowledgements

I am grateful to my supervisor, Stefan Weigert, for his help and guidance throughout my PhD. It has been a pleasure working together and I especially appreciate his patience and generosity of time. I would like to thank several members of staff in the Department of Mathematics, especially Paul Busch for his joint supervision during my first year at York, and Tony Sudbery for a proof of Theorem C.0.1 which he has kindly allowed me to reproduce here. I am also indebted to EPSRC for funding my research. Finally, I am grateful to my family, who have offered support and encouragement whenever necessary.

Author's declaration

I declare that the work presented in this thesis, except where otherwise stated, is based on my own research and has not been submitted previously for a degree in this or any other university. Parts of the work reported in this thesis have been published in:

D. McNulty and S. Weigert, "All mutually unbiased product bases in dimension 6", *J. Phys. A: Math. Theor.* **45**, 135307 (2012)

D. McNulty and S. Weigert, "The limited role of mutually unbiased product bases in dimension 6", *J. Phys A: Math. Theor.* **45**, 102001 (2012)

D. McNulty and S. Weigert, "On the impossibility to extend triples of mutually unbiased product bases in dimension six", *Int. J. Quan. Inf.* **10**, 1250056 (2012)

D. McNulty and S. Weigert, "Isolated Hadamard matrices from mutually unbiased product bases", *J. Math. Phys.* **53**, 122202 (2012)

Signed

Daniel McNulty

Chapter 1

Introduction

The formulation and development of quantum mechanics has brought forth a major revolution in our understanding of physics at the microscopic level. Intriguingly, the theory is far removed from the familiar classical picture of mechanics, where all dynamical variables of a system can be determined precisely. The revolutionary theory was developed independently in the twenties and early thirties of the last century: Schrödinger's wave mechanics established a differential equation with the use of operators while Heisenberg developed matrix mechanics and derived his uncertainty principle. Over the next half-century, an array of physicists and mathematicians, including Dirac, Born, Bohr, Jordon, von Neumann and many others, made significant contributions to the subject.

Abstractly, quantum mechanics involves linear operators acting on a Hilbert space (a complex vector space equipped with an inner product). A measurable quantity corresponds to a self-adjoint operator acting on the Hilbert space. Probably the most striking property of this theory is the probabilistic description of the states. In contrast to classical theory, not all dynamical variables of a state in a quantum mechanical system can simultaneously have sharp values. In other words, some dynamical variables will remain undetermined. Thus, quantum mechanics is a statistical theory providing probability distributions for the possible outcomes of a measurement of an observable. While there are still many issues today surrounding quantum mechanics and its interpretation, there is no doubting its power to make accurate experimental predictions.

The book by Isham [42] is recommended as a good introductory text to the subject, and further mathematical and interpretational discussions can be found in monographs by Mackey [59] and Bub [22].

This thesis is concerned with observables in quantum mechanics that exhibit *complementarity.* This is a property held by certain physical quantities for which a measurement of one observable implies maximum uncertainty about the possible outcome of a subsequent measurement of another observable. As an example, consider the Hilbert space $\mathcal{H} = \mathbb{C}^2$, in which a general qubit state ρ (a positive trace class operator of trace one) can be expressed as $\rho = \frac{1}{2}(I + \vec{r}.\vec{\sigma})$, where $\vec{r} \in \mathbb{R}^3$, $|\vec{r}| \leq 1$, I is the identity operator and $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$. The Pauli operators σ_x, σ_y and σ_z, together with I, form a self-adjoint operator basis. Consider a spin component observable $S^{\vec{a}}$ in the direction $\vec{a}$ and let " ± " label the two measurement outcomes. If the outcome is " + " then the spin direction is $\vec{a}$ and if the outcome is " − " the spin direction is $-\vec{a}$. The projection operators for this measurement, which project the state onto an eigenstate of the observable, are given by $S^{\vec{a}}(\pm) = \frac{1}{2}(I \pm \vec{a}.\vec{\sigma})$. Suppose that we have measured $S^{\vec{a}}$ and wish to predict the measurement outcome distribution of another spin component observable $S^{\vec{b}}$. For any state ρ, the *difference* between the outcome probabilities associated with $S^{\vec{a}}(+)$ and $S^{\vec{b}}(+)$ is given by $\frac{1}{2}|\vec{r}.(\vec{a} - \vec{b})|$, which is bounded above by $\frac{1}{2}\|\vec{a} - \vec{b}\|$. Thus, if $\vec{a}$ and $\vec{b}$ have similar directions, the outcome measurement distribution of $S^{\vec{a}}$ provides a fairly accurate estimate for the outcome measurement distribution of $S^{\vec{b}}$. However, if $\vec{a}$ is chosen *orthogonal* to $\vec{b}$ then we find that $\frac{1}{2}\|\vec{a} - \vec{b}\| = \frac{1}{\sqrt{2}}$. In this case, the outcome of a spin component measurement in direction $\vec{b}$ is completely unpredictable given that the system is in an eigenstate of spin in the orthogonal direction $\vec{a}$, i.e., the probability outcome distribution satisfies $\mathrm{tr}[\rho S^{\vec{b}}(+)] = \mathrm{tr}[\rho S^{\vec{b}}(-)] = \frac{1}{2}$ given $\rho = \frac{1}{2}(I + \vec{a}.\vec{\sigma})$. Thus, any two orthogonal spin component operators form a pair of complementary observables. For more detailed discussions on complementarity in quantum mechanics one can refer to [23, 38, 71].

One way to express complementarity for a pair of quantum mechanical observables is to say that their eigenstates form a pair of *mutually unbiased bases*: if a system resides in an eigenstate of one of these observables, there is a *uniform* probability distribution of finding the system in the eigenstates of the other observable. Formally, we say that two orthonormal bases $\mathcal{B}$ and $\mathcal{B}'$ of a finite-dimensional Hilbert space $\mathbb{C}^d$ are mutually unbiased (or MU for short) if and only if $|\langle\psi|\phi\rangle| = 1/\sqrt{d}$ for all $|\psi\rangle \in \mathcal{B}$ and all $|\phi\rangle \in \mathcal{B}'$. For example, the eigenstates of the three pairwise complementary spin operators σ_x, σ_y and σ_z form a set of three MU bases for which the overlap from vectors across different bases is $1/\sqrt{2}$.

The main purpose of this thesis is to investigate the *existence problem* of mutually unbiased bases in certain finite-dimensional Hilbert spaces $\mathbb{C}^d$. For arbitrary d it is well known that one can construct *at most* $(d+1)$ MU bases [97]. Furthermore, this upper bound is achieved when $d = p^n$, with p prime and $n \in \mathbb{Z}^+$. However, in every other dimension, *complete sets* of $(d+1)$ MU bases appear absent. While the problem still remains open, evidence suggests the existence of complete sets is unlikely for $d \neq p^n$ (we will often refer to these non-prime-power cases as composite dimensions). For the smallest composite dimension, $d = 6$, it is conjectured that only three of the possible seven MU bases exist [98].

Some interesting properties of operators which exhibit complementarity were first noticed by Schwinger in his paper "Unitary Operator Bases" [80]. Here, Schwinger investigates a pair of unitary operators U and V acting on a finite-dimensional Hilbert space $\mathbb{C}^d$, defined to cyclically permute (modulo d) the eigenstates of V and U, respectively. These operators satisfy the commutation relation $VU = e^{\frac{2\pi i}{d}} UV$ and generate a complete operator basis. In addition, the operators are maximally incompatible, i.e., their eigenstates form a pair of bases with constant overlap. When d is a prime number the operator basis yields a set of $d+1$ MU bases; an explicit construction was first given by Ivanovic in [43]. This was later generalised by Wootters and Fields to include prime-power cases [97]. The generalised construction depends on the existence of finite fields containing d elements and so the method does not apply when $d \neq p^n$.

Other constructions of complete sets have since been found [6, 31, 51]. A method by Bandyopadhyay *et al.* is based on finding maximally commuting subsets from a basis of orthogonal unitary matrices [6], and a construction by Klappenecker *et al.* uses finite fields and Galois rings [51]. Further studies on the relevence of finite fields for constructing MU bases can be found in [31,41,72,77,96].

Unfortunately, known constructions for complete sets are of little use in composite dimensions. It has been shown in [4] that generalised formulas based on the constructions given in [51,97] fail when the dimension d is composite. However, by factorising d into the form $d = p_1^{n_1} p_2^{n_2} \dots p_r^{n_r}$, where p_i is prime, $n_i \in \mathbb{Z}^+$ and $p_1^{n_1} < \dots < p_r^{n_r}$, one can construct at least $(p_1^{n_1} + 1)$ MU bases [51]. This bound is achieved by building bases in $\mathbb{C}^d$ from sets of MU bases in each prime-power subsystem. For most composite dimensions it appears likely that this lower bound is not exceeded, however, in certain square dimensions additional MU bases have been constructed using mutually orthogonal Latin squares [95].

The existence and construction of MU bases have some interesting links with other structures in mathematics. The most striking connection, found in [15], shows the existence of MU bases of the space $\mathbb{C}^d$ is *equivalent* to the existence of orthogonal Cartan subalgebras of the simple Lie algebra $sl_d(\mathbb{C})$. In fact, the existence problem for MU bases is equivalent to an older problem which conjectures that an orthogonal decomposition of $sl_d(\mathbb{C})$ exists if and only if d is a prime-power [55]. If this is true then complete sets of MU bases only exist in prime-power dimensions. Other analogous structures include affine planes (or mutually orthogonal Latin squares), which prove useful in the construction of MU bases [77], and complex Hadamard matrices [10]. These will be discussed thoroughly in Chapter 2.

Over the last decade substantial effort has been devoted to the existence problem in dimension six but the conjecture suggesting non-existence remains unproven. Various approaches attempt to find additional MU bases but to no avail. Extensive numerical searches suggest that no fourth basis exists [16,25], and it has been found that certain pairs and triples of MU bases cannot extend to a MU quadruple [34,45]. Other non-existence results rule out certain construction methods from yielding a complete set. For example, one can construct at most three MU bases from the partitioning of a nice error basis in dimension six [5], while in contrast, the method successfully generates complete sets of MU bases in prime and prime-power dimensions.

While results in dimension six are limited, most of the progress relies on restricting the search for MU bases in some way. For example, restricting the construction to nice error bases or limiting the search to include known pairs yields several non-existence results. In this thesis we focus on the product structure of the Hilbert space and limit our studies to bases which contain only *product* states. In particular, we investigate states of the form $|\psi, \Psi\rangle \equiv |\psi\rangle \otimes |\Psi\rangle$ in the space $\mathbb{C}^6$, with $|\psi\rangle \in \mathbb{C}^2$, and $|\Psi\rangle \in \mathbb{C}^3$. While product bases appear frequently in the studies of MU bases, their product structure is usually neglected. One of the few known results in dimension $d = 6$ is the impossibility to extend, by more than one further MU basis, the pair of bases consisting of the standard basis and its dual, the Fourier basis [34]. Another more recent result states that the Fourier family of Hadamard matrices in dimension six, together with the identity, does not extend to a MU quadruple [45]. These initial pairs, after non-local equivalence transformations, consist of *product* states only, a fact which has received little attention. Thus, on reflection it seems worthwhile to systematically study MU bases which contain only product states. In addition, this work will also complement studies of the entanglement structure of complete sets in prime-power dimensions where the product structure of MU bases plays an important role [58, 75, 93].

The structure of this thesis is as follows. In Chapter 2 we review progress made towards resolving the existence problem of complete sets of mutually unbiased bases in composite dimensions (i.e. non-prime-power cases), with particular focus on dimension six. We shall discuss several mathematical structures that are related to this problem, including orthogonal decompositions of simple Lie algebras, complex Hadamard matrices and affine planes. We will summarise all known *computational* and *analytic* results which provide evidence either for or against the conjecture that at most three MU bases exist in dimension six. Finally, we discuss a few well-known applications of MU bases, e.g. state tomography, quantum key distribution and the King's problem, and highlight possible workarounds if complete sets are found not to exist.

Chapters 3, 4 and 5 consist of three published papers on mutually unbiased product bases. In Chapter 3 we start by deriving an exhaustive list of *product* bases of the space $\mathbb{C}^2 \otimes \mathbb{C}^3$, inequivalent under local equivalence transformations. By imposing the condition for a product basis to be MU to a product vector we arrive at two results important to enumerate all pairs and triples of MU product bases. We then give a complete classification of all MU product bases in dimension six. To illustrate our method and confirm various known results we also provide a complete classification of all MU product bases of the space $\mathbb{C}^2 \otimes \mathbb{C}^2$. The classification in dimension six reveals four families of pairs of MU product bases: a four-parameter family; two pairs containing two-parameters; and a single parameter-independent pair. In addition, there exist only two triples of MU product bases. As a consequence of this classification, and with some help from a computer-aided search given by Grassl in [34], it follows that no MU product triple is part of a complete set of seven MU bases.

In Chapter 4 we provide a stronger non-existence result for MU product bases in dimension six by proving that if a complete set of seven MU bases exist, it contains at most *one* product basis. The proof relies on the classification of pairs of MU product bases derived in the previous chapter and two computer algebraic calculations given in [45] and [18]. In particular, we show that all pairs of MU product bases are equivalent under non-local unitary transformations to just two types. Written in matrix form, these pairs both contain the identity matrix together with either the two-parameter Fourier family $F_6(a, b)$ or the isolated matrix S_6. A computational search given by Jaming *et al.*, which is made exact by using rigorous error bounds, shows that the pair containing the identity matrix and Fourier family cannot extend to a quadruple of MU bases [45]. A search for vectors MU to the identity matrix and S_6 rules out the extension of this pair beyond a MU triple. Thus, since all MU product pairs are equivalent to bases known to be unextendible, it follows that a complete set will contain only one product basis, the standard canonical basis.

The non-existence results we have so far derived, while rigorous, rely in some way on computer algebraic manipulations. In Chapter 5, we overcome this deficiency by proving two analytic non-existence results. Both statements are weaker than the main result of Chapter 4 but they nevertheless offer an additional perspective and complement the few analytic results that already exist. The first result is a proof that no vector is MU to a triple of MU product bases in dimension six. The proof relies on some simple mathematical techniques which exploit the tensor product structure of the Hilbert space $\mathbb{C}^2 \otimes \mathbb{C}^3$. The second result is slightly stronger and considers *constellations* of MU product states rather than bases. A MU constellation is a set containing orthogonal and MU states. For example, any subset of a set of MU bases is a MU constellation. The product constellation we consider contains 16 product states: two bases and a set of four orthogonal states. We show that any product constellation of this type cannot be extended to a complete set of seven MU bases.

In Chapter 6 we shift our focus from the existence problem of MU bases in dimension six to the construction of complex Hadamard matrices in composite dimensions. The two structures are closely related since a set of MU bases can be represented by a set of complex Hadamard matrices. A square matrix H of order d is a complex Hadamard matrix if it is unitary, $HH^\dagger = I$, and if its elements have equal modulus. This definition generalises the concept of a *real* Hadamard matrix where the matrix elements are limited to the values $\pm 1/\sqrt{d}$. The first known construction of such matrices is due to Sylvester [83], while they take their name from Hadamard who found that the absolute value of the determinant of a unitary matrix achieves its maximum if all its matrix elements have the same modulus [36]. Since then, complex Hadamard matrices have made their appearance in various branches of both mathematics and physics. For example, they relate to the problems of finding bi-unitary sequences and cyclic n-roots [13], they can be useful in constructing certain *-subalgebras of finite von Neumann algebras [73], and error correcting codes [2]. They also have applications in quantum information, representing an important ingredient in teleportation and dense coding schemes [92], and they are closely linked to mutually unbiased bases [80]. For a detailed overview of their applications, see [2, 39].

In view of their many uses, a complete classification of complex Hadamard matrices would be highly desirable but it has not yet been achieved. All complex Hadamard matrices, up to equivalence, are known for dimensions $d \leq 5$ [35, 91], but their classification remains incomplete for higher dimensions. General construction methods exist in composite dimensions [28, 40], and continuous families of complex Hadamard matrices have been obtained from so-called *parameterisations* of known Hadamard matrices [28–30, 61]. There has also been some success in finding continuous families of complex Hadamard matrices for certain prime dimensions [70]. A survey of known complex Hadamard matrices is given in [88] for $d \leq 16$, with an updated online catalogue provided by [21].

Chapter 6 contains a new construction method for complex Hadamard matrices of order $d = pq$, with p, q prime, based on pairs of MU product bases of the same dimension. This technique stems from our classification of all MU product bases in dimension six given in Chapter 3. Furthermore, we show that for a certain choice of bases, new examples of *isolated* complex Hadamard matrices appear. A complex Hadamard matrix is isolated if the upper bound on the dimensionality of the set of Hadamard matrices stemming from the matrix is zero, i.e. it is disconnected from any continuous set. We demonstrate the method for $d < 100$, and construct at least 12 new isolated matrices from order 9 to 91. All of the tested dimensions (except $d = 4$) result in at least one isolated Hadamard matrix. This is in contrast to the discovery of most other isolated matrices, which are usually found through numerical searches and occur quite sporadically.

We conclude this thesis in Chapter 7 with a brief discussion of our main results.

Chapter 2

The MUB problem in $d = 6$

2.1 Orthogonal decompositions of $sl_d(\mathbb{C})$

The unsolved problem of whether complete sets of MU bases exist in arbitrary dimensions is connected, somewhat surprisingly, to an analogous problem involving orthogonal decompositions of Lie algebras. In fact, the conjectured non-existence of complete sets in composite dimensions is equivalent to a much older conjecture that the simple Lie algebra $sl_d(\mathbb{C})$ admits an orthogonal decomposition only if d is a prime-power [55]. In this section we summarise the *equivalence* of the existence of MU bases for arbitrary dimension d with orthogonal Cartan subalgebras of $sl_d(\mathbb{C})$ as shown in [15] and highlight a consequence for dimension six.

Suppose that $\mathcal{L}$ is the simple Lie algebra $sl_d(\mathbb{C})$ consisting of all traceless complex matrices of order d. A *Cartan subalgebra* $\mathcal{H}$ of $\mathcal{L}$ is a maximal subspace that is self-normalising, i.e. if $[g, h] \in \mathcal{H}$ for all $h \in \mathcal{H}$, then $g \in \mathcal{H}$. The *Killing form* $K(x, y)$ is defined as

$$K(x, y) = \mathrm{tr}(\mathrm{ad}_x \cdot \mathrm{ad}_y), \tag{2.1}$$

where $\mathrm{ad}_x : \mathcal{L} \to \mathcal{L}$, for some element $x \in \mathcal{L}$, is the *adjoint endomorphism* with $\mathrm{ad}_x(z) = [x, z] = xz - zx$ for all $z \in \mathcal{L}$. The Killing form is non-degenerate on $\mathcal{L}$ as well as on the restriction to any Cartan subalgebra $\mathcal{H}$. Thus, two Cartan subalgebras $\mathcal{H}_i$ and $\mathcal{H}_j$ are *orthogonal* with respect to the Killing form if $K(\mathcal{H}_i, \mathcal{H}_j) = 0$.

The following theorem summarises the equivalence between sets of MU bases and orthogonal Cartan subalgebras, first noticed in [15].

Theorem 2.1.1. *A set of μ MU bases $\mathcal{B}_1, \ldots, \mathcal{B}_\mu$ of $\mathbb{C}^d$ exists if and only if a set of μ pairwise orthogonal Cartan subalgebras $\mathcal{H}_1, \ldots, \mathcal{H}_\mu$ of $sl_d(\mathbb{C})$, closed under the adjoint operation, exists.*

This equivalence can be understood as follows. One can construct a Cartan subalgebra $\mathcal{H}$ from an orthonormal basis $\mathcal{B} = \{|\psi_1\rangle, \ldots, |\psi_d\rangle\}$ if $\mathcal{H}$ is defined as the linear subspace of $sl_d(\mathbb{C})$ consisting of all traceless matrices that are diagonal in $\mathcal{B}$. Any element $x \in \mathcal{H}$ can be written as $x = \sum_i a_i |\psi_i\rangle\langle\psi_i|$, with $\sum_i a_i = 0$. By associating each Cartan subalgebra $\mathcal{H}_i$ with a mutually unbiased basis $\mathcal{B}_i$ in this way, it is straightforward to show that two Cartan subalgebras $\mathcal{H}_i$ and $\mathcal{H}_j$ are *orthogonal* with respect to the Killing form.

To construct an orthonormal basis $\mathcal{B}$ from a Cartan subalgebra $\mathcal{H}$, one takes the common eigenvectors of all the matrices in $\mathcal{H}$ as the elements of $\mathcal{B}$. To show that two bases $\mathcal{B}_i$ and $\mathcal{B}_j$ which correspond to two orthogonal Cartan subalgebras $\mathcal{H}_i$ and $\mathcal{H}_j$ are mutually unbiased, one simply assumes the opposite, leading to a contradiction of the orthogonality condition.

Since any Cartan subalgebra, closed under adjoint operation, has a basis of unitary matrices that is orthogonal with respect to the Killing form, this construction of MU bases is equivalent to a construction given in [6] which depends on collections of maximally commuting classes of unitary error bases. A *maximally commuting basis* $\mathcal{C}$ of unitary matrices, orthogonal with respect to the trace inner product, is a basis of complex $d \times d$ matrices which can be partitioned into classes of $d-1$ commuting matrices $\mathcal{C}_i$ such that $\mathcal{C} = I \cup \mathcal{C}_1 \cup \ldots \cup \mathcal{C}_{d+1}$, with I the identity matrix. If such a partition occurs, then a complete set of MU bases can be constructed. Furthermore, a set of μ MU bases in $\mathbb{C}^d$ is equivalent to a set of μ maximally commuting classes $\mathcal{C}_1, \ldots, \mathcal{C}_\mu$, with each class containing d commuting unitary matrices such that the elements in $\mathcal{C}_1 \cup \ldots \cup \mathcal{C}_\mu$ are orthogonal [6].

From Theorem 2.1.1 it is clear that a complete set of $d+1$ MU bases exists if and only if one can find a set of pairwise orthogonal Cartan subalgebras $\mathcal{H}_1, \ldots, \mathcal{H}_d$ of the Lie algebra $\mathcal{L}$. Such a set forms an *orthogonal decomposition* of $\mathcal{L}$ and, as a vector space, can be written as a direct sum

$$\mathcal{L} = \mathcal{H}_1 \oplus \ldots \oplus \mathcal{H}_d. \tag{2.2}$$

While it has been shown that orthogonal decompositions exist for $\mathcal{L} = sl_d(\mathbb{C})$ when d is a prime-power, their existence in other dimensions in unknown. It is conjectured that orthogonal decompositions of this kind exists only in prime-power cases.

A consequence of the equivalence of MU bases to orthogonal Cartan subalgebras of $sl_d(\mathbb{C})$ is the following result given in [15].

Theorem 2.1.2. *In dimension six no more than three MU bases exist that are monomial.*

A set of MU bases is *monomial* if the set of maximally commuting matrices, which yield the MU bases from their eigenvectors, contains only monomial matrices, i.e. matrices that have only one non-zero element in each row and column. Theorem 2.1.2 follows directly from a result proved in [55] which shows that no more than three monomial, pairwise orthogonal, Cartan subalgebras of the Lie algebra $sl_6(\mathbb{C})$ exist. This restriction seems quite severe in light of a result in [33] that every known construction of complete sets of MU bases, including those given in [6, 97], is monomial.

2.2 Complex Hadamard matrices

A complex Hadamard matrix of order d is a generalisation of a real Hadamard matrix which is a square, unitary matrix, with entries consisting of $\pm 1/\sqrt{d}$. The generalisation allows one to drop the restriction of real entries to those with modulus $1/\sqrt{d}$. Our focus on complex Hadamard matrices is motivated by their close correspondence to mutually unbiased bases; any pair of MU bases in a finite dimensional Hilbert space $\mathbb{C}^d$ can be represented by a complex Hadamard matrix H of order d. To see this, we can write a pair of MU bases as a pair of unitary matrices B_1 and B_2 where the columns within each matrix represent orthonormal states. By performing a unitary transformation on both matrices such that one is mapped to the identity matrix, the second becomes a Hadamard matrix H. Since the columns of H are mutually unbiased to the columns of the identity matrix, their elements have equal modulus, i.e. $|h_{ij}| = 1/\sqrt{d}$. Thus, by searching for Hadamard matrices of a particular order, one is also searching for pairs of *complementary* bases. A complete classification of Hadamard matrices (pairs of complementary bases) is given for $d \leq 5$ [35] and while these matrices exist in all dimensions, complete classifications are still unknown. We will discuss this open problem for $d = 6$ later in this section.

In the classification of Hadamard matrices, the ordering of the columns and their overall phase factors are not important. Therefore, we can multiply a Hadamard H from the left by a permutation matrix P_1 and a unitary diagonal matrix D_1 and the resulting matrix HD_1P_1 is regarded as equivalent to H. Similarly, equivalence is also maintained if we multiply H from the left with permutation and diagonal matrices. Thus, two Hadamard matrices H and K are equivalent, i.e. $H \sim K$, if they satisfy $H = P_1D_1KD_2P_2$. As a consequence, a Hadamard matrix is usually expressed in its dephased form with the first row and column having elements $h_{i1} = h_{1j} = 1/\sqrt{d}$.

It can be difficult to deduce whether two matrices are (in)equivalent but a useful test given in [35] can often show that two matrices are *inequivalent*. This approach involves constructing the Haagerup set $\Lambda(H)$ of the complex Hadamard matrix H,

$$\Lambda(H) = \{h_{ij}h_{kl}h^*_{il}h^*_{kj} : i, j, k, l = 1, \ldots, d\}, \tag{2.3}$$

where h^*_{ij} denotes the complex conjugation of h_{ij}. The Haagerup set is invariant under equivalence transformations so if two matrices H and K have *different* Haagerup sets, they are *inequivalent*.

It is usually the case that a Hadamard matrix is contained in a set of Hadamard matrices where the elements depend on continuous parameters. An *affine* family of Hadamard matrices is a set $H(\mathcal{R})$ stemming from a Hadamard matrix H of order d, where

$$H(\mathcal{R}) = \{H \circ \mathrm{EXP}(i \cdot R) : R \in \mathcal{R}\}, \tag{2.4}$$

and $\mathcal{R}$ is a subspace of all real matrices of order d with zeros in the first row and column. The notation $\circ$ is the entrywise product of matrices (the Hadamard product), and $\mathrm{EXP}(.)$ is the entrywise exponential function acting on a matrix. A family which does not fall into an affine set is called *non-affine*.

An upper bound on the number of free parameters for the set of matrices stemming from H is given by the *defect* of H, $d(H)$. This bound was derived in [88] and is useful when a matrix is *isolated*: a Hadamard matrix H is isolated if its defect is zero. In other words, all Hadamard matrices within a neighbourhood of H are equivalent. We can calculate the defect by introducing phases into the *core* of the matrix, where the core consist of all elements $h_{ij} \neq h_{1,j}, h_{i,1}$, and solving the unitary condition up to first order from the Taylor series (see [10] for an example). The defect corresponds to the number of free parameters remaining. In most cases when d is large, a computer program is necessary for the calculation.

An alternative method to determine if a matrix is isolated is the *span condition* presented in [66]: if H is a Hadamard matrix and the dimension of the vector space $\mathrm{span}\{uv - vu : u \in \mathcal{D}, v \in H^*\mathcal{D}H\}$ is $(d-1)^2$, then H is *isolated.* Here, $\mathcal{D}$ is the algebra of diagonal matrices and H^* denotes the complex conjugate of H. It is presently unknown if isolation is equivalent to the span condition, i.e. can a matrix have non-zero defect and not be part of any family?

While the defect provides an upper bound on the dimensionality of the Hadamard family, it is not true that this bound is always reached. The definition is based on first order calculations of the unitary condition and investigating higher order terms can lead to a more precise upper bound [8]. As an example, the Fourier matrix F_d, with $f_{ij} = \omega^{ij}/\sqrt{d}$ and $\omega = e^{2\pi i/d}$, has a defect given by

$$d(F_d) = \sum_{n=1}^{d-1} (\gcd(n, d) - 1). \tag{2.5}$$

This is a strict upper bound when d is a prime-power, but the dimension of the largest smooth family stemming from F_d is strictly *less* than the defect for $6 < d \leq 100$ when d is not a prime or prime-power [8]. The $d = 6$ case turns out to be special: the defect of F_6 is four and evidence suggests the existence of a four-parameter family containing F_6 [8, 82]. Furthermore, it seems that the bound on the dimension of a smooth family stemming from the Fourier matrix depends on the prime decomposition of d. It has so far not been possible to find an exact bound for arbitrary d but it has been conjectured that if $d = p_1 p_2^2$ there is a non-linear family of Hadamard matrices stemming from F_d which has $3p_1p_2^2 - 3p_1p_2 - 2p_2^2 + p_2 + 1$ free parameters [8]. Since we know that Hadamard matrices correspond to pairs of complementary bases, this result suggests the geometry of the quantum state space depends heavily on the number theoretic properties of the dimension.

2.2.1 The classification problem for $d = 6$

Considerable effort has been devoted to the problem of classifying complex Hadamard matrices of order six. Its recent prominence has been motivated primarily by the search for a complete set of MU bases in dimension six; a successful classification would narrow down the state space where these bases exist to a size in which a computational search is possible. While the classification remains incomplete, we will summarise the progress that has been made so far.

For every non-prime dimension there exists an affine Fourier family of Hadamard matrices and its transpose family. In dimension six, these are the two-parameter families denoted by $F_6^{(2)}$ and $(F_6^{(2)})^T$, respectively. The discovery of other complex Hadamard matrices has been quite staggered, with individual examples found and later extended or connected by one- and two-parameter families. In most cases, the methods of construction focus on restricting the search to various special cases, e.g. self-adjoint or symmetric matrices. For example, the classification of all self-adjoint complex Hadamard matrices of order six yields a non-affine one-parameter family found in [9], and a non-affine one-parameter family of symmetric matrices was derived in [63]. More general two-parameter families, which contain the one-parameter families as a subset, were later discovered in [47, 85].

Further progress was made towards a classification by the discovery of an elegant three-parameter family $K_6^{(3)}$, derived in [49], that encompasses all previously known one- and two-parameter families. The three-parameter family was found by investigating matrices that are H_2*-reducible*; a property whereby all (2×2) submatrices of a (6×6) matrix are Hadamard [48]. Surprisingly, every Hadamard matrix of order six is equivalent to a matrix where *all* or *none* of the nine 2×2 submatrices are Hadamard. It is simple to check the H_2-reducibility property since a matrix of order six is H_2-reducible if and only if its dephased form contains an element equal to (-1). Note that for convenience we also refer to matrices as Hadamard if their elements have modulus 1 rather than $1/\sqrt{d}$.

To construct $K_6^{(3)}$, one starts with a general dephased block matrix H_6 of nine (2×2) submatrices. By requiring that H_6 is H_2-reducible and using the unitary and unimodularity constraints on its elements, a complete classification of all H_2-reducible Hadamard matrices is covered by the three-parameter set

$$K_6^{(3)} = \begin{pmatrix} F_2 & Z_1 & Z_2 \\ Z_3 & \frac{1}{2}Z_3AZ_1 & \frac{1}{2}Z_3BZ_2 \\ Z_4 & \frac{1}{2}Z_4BZ_1 & \frac{1}{2}Z_4AZ_2 \end{pmatrix}, \tag{2.6}$$

as described in [49]. The (2×2) matrix

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{12} & -A_{11} \end{pmatrix} \tag{2.7}$$

has elements

$$A_{11} = \frac{1}{2} + i\frac{\sqrt{3}}{2}(\cos\theta + e^{-i\phi}\sin\theta), \tag{2.8}$$

$$A_{12} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}(-\cos\theta + e^{i\phi}\sin\theta), \tag{2.9}$$

with $\theta, \phi \in [0, \pi)$ and $B = -F_2 - A$. The submatrices $Z_i = \begin{pmatrix} 1 & 1 \\ z_i & -z_i \end{pmatrix}$ for $i = 1, 2$

and $Z_i = \begin{pmatrix} 1 & z_i \\ 1 & -z_i \end{pmatrix}$ for $i = 3, 4$ contain parameters z_i satisfying $|z_i| = 1$ which are related via the Möbius transformations $z_3^2 = \mathcal{M}_A(z_1^2)$, $z_3^2 = \mathcal{M}_B(z_2^2)$, $z_4^2 = \mathcal{M}_A(z_2^2)$ and $z_4^2 = \mathcal{M}_B(z_1^2)$, where $\mathcal{M}(z) = \frac{\alpha z - \beta}{\bar{\beta} z - \bar{\alpha}}$, $\alpha_A = A_{12}^2$, $\beta_A = A_{11}^2$, $\alpha_B = B_{12}^2$ and $\beta_B = B_{11}^2$. By choosing $z_1 = e^{i\lambda}$, say, the remaining three parameters z_i are constrained by the Möbius transformations and the resulting three-parameter family is $K_6(\theta, \phi, \lambda)$.

The parameterisation in $K_6^{(3)}$ is somewhat different to those used in the smaller one- and two-parameter families, so connections between $K_6^{(3)}$ and its subfamilies are difficult to see. However, at the limit $\theta = 0$, the Fourier family $F_6^{(2)}$ is recovered by taking z_1 and ϕ as the free parameters. Similarly $(F_6^{(2)})^T$ is recovered if z_3 and ϕ are the free parameters.

Although the three-parameter family goes some way towards completing the classification, numerical evidence in [82] suggests the existence of a four-parameter family. By performing infinitesimal shifts of phases in the Fourier matrix, the unitary condition of the Hadamard matrix is preserved while moving away along four directions. This was confirmed in [87] where a construction was given for a four-parameter set $G_6^{(4)}$. The matrix elements of $G_6^{(4)}$ are given by algebraic functions of roots of sextic polynomials, however it has not been possible to express these functions in terms of closed expressions. The construction is non-trivial and quite complicated so we refer the reader to [87] for all the details. The matrix takes the form

$$G_6(a,b,c,d) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & a & b & e & s_1 & s_2 \\ 1 & c & d & f & s_3 & s_4 \\ 1 & g & h & * & * & * \\ 1 & t_1 & t_3 & * & * & * \\ 1 & t_2 & t_4 & * & * & * \end{pmatrix} \equiv \begin{pmatrix} E & B \\ C & D \end{pmatrix}, \tag{2.10}$$

where E, B, C and D are (3×3) submatrices. The elements of B and C are found from the orthogonality conditions of the first three rows and columns of $G_6^{(4)}$ as well as other results involving *Haagerup's trick* [35], but the solutions are by no means trivial.

Once this is complete, the elements of D can be determined since $D = -CE^\dagger(B^{-1})^\dagger$, where $\dagger$ denotes the conjugate transpose. Once the elements e, f, g, h, s_i and t_i – all dependent on a, b, c and d – have been calculated, it is then decided algorithmically if the submatrix E can be embedded in the Hadamard matrix $G_6^{(4)}$. The detailed steps of the construction are spelled out in [87] and a Mathematica script which finds random examples based on this construction is provided in [21].

Whilst we have so far only considered matrices that are contained in continuous families, isolated examples may also occur. This is indeed true in dimension six where one isolated matrix, the symmetric Hadamard matrix S_6, is known. It has been found independently in various derivations but it is unknown if other such isolated examples exist. Its first construction was given by Butson in [24] where he provides a technique to construct matrices of order $2p$ which contain only p-th roots of unity, when p is prime. For $p = 3$, the construction leads to a matrix consisting of third roots of unity only, namely S_6. Other derivations have been found using numerical searches [89], symmetric conditions [63], or MU product bases (see Chapter 4).

It has been conjectured in [87] that every complex Hadamard matrix of order six is equivalent to a member of either $G_6^{(4)}$, $K_6^{(3)}$ or S_6. The relationship between $G_6^{(4)}$ and $K_6^{(3)}$ is not fully understood; one expects that $K_6^{(3)}$ is a subset of $G_6^{(4)}$ but it is not even known if the Fourier family is contained in $G_6^{(4)}$. If one is equipped with a proof of this conjecture, it may indeed be possible to decide how many MU bases the space $\mathbb{C}^6$ can accommodate. This would follow in analogy to a proof by an exhaustive computer search in [45] which excludes the Fourier family $F_6^{(2)}$ (and its transpose) from appearing in a hypothetical set of seven MU bases.

2.3 Affine planes and Latin squares

Another object in mathematics with striking similarities to sets of MU bases is an affine plane. These particular geometric structures consist of points and lines which satisfy the following three axioms: any two points have exactly one line in common; for any line and additional point there is a unique line through this point and disjoint (parallel) from the given line; and finally, there exists at least three noncollinear points. This being the case, an affine plane of order d contains d^2 points and $d(d+1)$ lines, with each line containing d points. The lines of an affine plane can be partitioned into $d+1$ sets, called *striations*, each containing d parallel lines. Any pair of non-parallel lines intersect at only one point.

It is known that affine planes of order d exists if d is a prime or prime-power, however, for certain composite dimensions, e.g. $d = 6$, affine planes do not exist. In fact, the Bruck-Ryser theorem states that no affine plane of order d exists if $d-1$ or $d-2$ is divisible by four and d is not the sum of two squares [20]. Numerical computations have also ruled out their existence for $d = 10$ [56].

These results bear a striking resemblance to the MU problem, and the following conjecture has been made in light of these similarities [78]: *The non-existence of a projective plane of the given order d implies that there are less than $d+1$ MU bases in the corresponding Hilbert space $\mathbb{C}^d$, and vice versa.* A projective plane is used here instead of an affine plane, but the two objects are essentially the same. One can construct an affine plane from a projective plane by removing a single line and all its containing points.

While no rigorous association between affine planes and MU bases is known, it has been suggested in [96] to treat the lines as projection operators P_i, projecting onto orthogonal quantum states. A set of d parallel lines then corresponds to a basis of d orthogonal projection operators satisfying $\sum_i P_i = 1$, and two non-parallel lines with associated projection operators P_i and Q_j satisfy $tr(P_iQ_j) = 1/d$. Thus, the $d+1$ *striations* of an affine plane correspond to a set of $d+1$ MU bases. An obvious question subsequently arises about the role of the d^2 points in such a correspondence. In [96], a point α is chosen to represent a Hermitian operator A_α/d such that: (i) $tr(A_\alpha/d) = 1/d$; (ii) $tr(A_\alpha/d)(A_\beta/d) = \delta_{\alpha\beta}/d$; and (iii) $\sum_\alpha(A_\alpha/d) = P_i$. Unfortunately, in this scheme the existence of $d+1$ striations does not imply the existence of a complete set of MU bases since there is no known construction of the operators A_α.

Interestingly, affine planes are also analogous, in some sense, to SIC-POVMs. By switching the roles of points and lines in the geometry, i.e. an object with d^2 lines and

$d(d+1)$ points, a SIC-POVM mirrors the geometric structure of an affine plane [96].

An affine plane can also be represented by a set of orthogonal Latin squares. A Latin square of order d is an array of $d \times d$ integers $\{0, \ldots, d-1\}$ such that each number appears exactly once in each row and column. Two Latin squares L and L' are orthogonal if all ordered pairs of elements (L_{ij}, L'_{ij}) are distinct. For every prime and prime-power d, there exists a complete set of $d-1$ mutually orthogonal Latin squares (MOLS), as follows from the existence of affine planes.

A set of ℓ mutually orthogonal Latin squares can be extended to an *augmented* set of MOLS which include two additional (non-Latin) squares A and B such that $A_{ij} = i$ and $B_{ij} = j$. An example of an augmented set of MOLS in $d = 3$ is given by

$$\begin{array}{ccc} 0 & 1 & 2 \\ 0 & 1 & 2 \\ 0 & 1 & 2 \end{array} \qquad \begin{array}{ccc} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 2 & 2 & 2 \end{array} \qquad \begin{array}{ccc} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{array} \qquad \begin{array}{ccc} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{array} \tag{2.11}$$

where the last two squares are Latin and all four are mutually orthogonal. Each square from an augmented set of MOLS corresponds to a striation of an affine plane, with the points on a line relabelled by distinct integers.

An augmented set of orthogonal Latin squares of size $\ell + 2$ is equivalent to a combinatorial design known as a *net* which consists of $\ell + 2$ rows. The algorithm which translates an augmented set of $\ell + 2$ MOLS to a *net design* is given in [68]. The corresponding net design can be written as a table whereby each row containing d^2 integers separates into d cells of size d. The numbers contained in one cell of a given row are distributed evenly among all cells of any other row. The correspondence between MU bases and net designs results from linking the cell elements to the exponents of the Heisenberg-Weyl cyclic shift (modulo d) and phase operators X and Z, respectively, defined as

$$X|j\rangle = |j+1\rangle \qquad \text{and} \qquad Z|j\rangle = \omega^j |j\rangle, \tag{2.12}$$

where $\omega = e^{2\pi i/d}$ is a d-th root of unity and $\{|j\rangle\}$ is the standard basis with $j = 0 \ldots d-1$. If d is prime, one can construct a complete set of $(d+1)$ MU bases from the eigenbases of the operators Z and $X(Z)^k$ for $0 \leq k \leq d-1$ [6].

One useful consequence of the link between these two problems was a new construction of MU bases in certain *square* dimensions found in [95]. When the dimension of the Hilbert space is neither prime nor prime-power and its prime factorisation is given by $d = p_1^{n_1} \dots p_r^{n_r}$, one can always find at least $\min_i(p_i^{n_i} + 1)$ MU bases in $\mathbb{C}^d$ by taking the tensor products of MU bases from the space corresponding to each prime-power factor [51]. However, if the dimension is square, i.e. $d = s^2$, and the augmented set of MOLS of order s is greater than $\min_i(p_i^{n_i} + 1)$, one can find more MU bases than the lower bound. The first example occurs when $d = 26^2$, where the number of MOLS is at least four and so one can construct six MU bases, one more than the minimum five bases.

In dimension six no two MOLS exist and the best one can do, based on the construction given in [68], is to find three MU bases from the augmented set of three MOLS. As we have already seen with the existence of affine planes, if the two problems are equivalent, then this is sufficient to prove the inexistence of a complete set in dimension six.

Some caution should be taken with the proposed equivalence of affine planes and MU bases since unexpected differences appear between these structures [91]. The differences arise when one considers mutually unbiased *constellations*: a set of vectors for which pairs can be either orthogonal or mutually unbiased. For example, a set of two bases and four orthonormal states of the space $\mathbb{C}^6$ is a MU constellation when all non-orthogonal vectors in the constellation are mutually unbiased.

As we shall discuss later, a numerical search presented in [16] is unable to find a MU constellation consisting of three MU bases together with four orthogonal states. However, the largest *affine constellation* to exist contains three striations, each with six lines, and an additional set of four parallel lines. An affine constellation consists of sets of points and lines such that any two lines within a set do not intersect, and any pair of lines from different sets have one point in common. Thus, if an affine constellation does not exist, then neither will an affine plane. If there is some deep underlying connection between affine planes and MU bases, for example with parallel lines corresponding to orthonormal bases and intersecting ones to MU states [96], one would expect the structure of affine and MU constellations to be similar, which seems not to be the case.

2.4 Analytically searching for MU bases

We have so far covered several analytic results regarding MU bases in composite dimensions. These include: (i) the equivalence of complete sets of MU bases with orthogonal decompositions of simple Lie algebras $sl_d(\mathbb{C})$; (ii) the non-existence of four monomial MU bases in dimension six, i.e. Theorem 2.1.2; (iii) the construction of a three-parameter family of H_2-reducible complex Hadamard matrices $K_6^{(3)}$; and (iv) a construction of MU bases in square dimensions, $d = s^2$, based on Latin squares, which for some values of s yields more MU bases than expected. We now summarise several other known analytic results on mutually unbiased bases valid for non-prime-power dimensions.

2.4.1 Nice error bases

The construction of MU bases is equivalent to the partitioning of a maximally commuting basis (unitary error basis) of unitary matrices in the Hilbert space $\mathbb{C}^{d\times d}$ into subsets of maximally commuting matrices. This was briefly discussed in Sec. 2.1. By considering a specific type of unitary error basis, namely a *nice error basis*, there is a limit on the number of MU bases one can constructed [5]. A nice error basis is defined as follows [15]:

Definition 2.4.1. *Let $\mathcal{G}$ be a group of order d^2 with identity element e. A set $\mathcal{N} = \{U_g : g \in \mathcal{G}\} \subset \mathbb{C}^{d\times d}$ of unitary matrices is a nice error basis if*

1. *U_e is the identity matrix,*
2. *$tr(U_g) = 0$ for all $g \in \mathcal{G} \setminus \{e\}$,*
3. *$U_g U_h = \omega(g,h) U_{gh}$ for all $g, h \in \mathcal{G}$,*

where $\omega(g,h) \in \mathbb{C}$ has modulus one.

As a simple example, consider $d = p^k$, for prime p, and take the index group as $\mathcal{G} = \mathbb{Z}_p^k \times \mathbb{Z}_p^k$ where $\mathbb{Z}_p = \{0, \ldots, p-1\}$ such that $(x,z) = (x_1, \ldots, x_k, z_1, \ldots, z_k) \in \mathbb{Z}_p^k \times \mathbb{Z}_p^k$. A nice error basis $\mathcal{N}$ can be constructed from the Heisenberg-Weyl operators X and Z, defined in Eq. (2.12), such that

$$\mathcal{N} = \{U^{(x,z)} : (x,z) \in \mathbb{Z}_d^k \times \mathbb{Z}_d^k\}, \tag{2.13}$$

with

$$U^{(x,z)} = X^{x_1} Z^{z_1} \otimes \ldots \otimes X^{x_k} Z^{z_k}. \tag{2.14}$$

We now summarise the main result in [5] which places a limit on the number of MU bases one can construct from a nice error basis.

Theorem 2.4.2. *Let $\mathcal{N}$ be a nice error basis of $\mathbb{C}^{d \times d}$ then the maximum number of mutually unbiased bases that can be obtained by partitioning a subset of $\mathcal{N}$ into maximally commuting classes is at most $min_i(p_i^{n_i} + 1)$ where $d = p_1^{n_1} \ldots p_r^{n_r}$. This bound is achieved iff d is a prime or prime-power, and in this case the unitary error basis is equivalent to the basis given in Eq. (2.13).*

An obvious consequence is that only three nice MU bases can be constructed from a nice error basis in dimension six. However, this does not rule out the existence of additional bases which may be mutually unbiased to three nice MU bases. For $d = p^k$, the nice error basis given in Eq. (2.13) can be partitioned into $d+1$ maximally commuting classes, thus, a complete set of $d+1$ MU bases is derived. Notice that by restricting ourselves to unitary error bases which form a complete collection of maximally commuting classes and MU bases, the niceness of the unitary error basis implies monomiality via Theorem 2.4.2. In general, however, without the requirement of a complete partitioning of the error basis, niceness and monomiality do not imply each other [53].

One important observation pointed out in [15] is that an “incomplete” set of MU bases constructed from Latin squares [68] is *not* contained in a nice error basis. However, the bases found in [68] are monomial, and every known complete set of MU bases is monomial *and* obtained by partitioning nice error bases [33].

2.4.2 Entanglement in MU bases

The role of entanglement in sets of MU bases has been studied in [93]. In particular, the entanglement content of complete sets of MU bases is investigated for a bipartite quantum system of dimension $d = d_A d_B$, where d_A and d_B are prime, and $d_A \leq d_B$. It is found that any complete set must contain a fixed amount of entanglement $\mathcal{E}$ given by

$$\mathcal{E} = d_A d_B (d_A + d_B). \tag{2.15}$$

The measure of entanglement used here is a function of the linear entropy of a reduced density operator $\rho_A = tr_B(\rho)$ given by the purity $tr(\rho_A^2)$. The purity obtains its minimum value of $1/d_A$ when the state is maximally entangled, and its maximum of unity when the state is separable. A proof of the fixed entanglement content makes use of *complex projective 2-designs*; a complete set of MU bases is an example of a complex projective 2-design [52]. We shall discuss this concept more thoroughly in Sec. 2.6.

As a consequence of Eq. (2.15), complete sets must include both entangled *and* product states. In other words, the fixed entanglement content makes it impossible for a complete set to contain only entangled states *or* product states. However, the distribution of entanglement within a complete set is arbitrary. For example, suppose that for a bipartite quantum system of dimension $d = d_A d_B$ with $d_A < d_B$, we have a set of $d_A + 1$ MU product bases, then the remaining bases of a (hypothetical) complete set of $d_A d_B + 1$ bases must contain only entangled states.

In dimension six, where $d_A = 2$ and $d_B = 3$, the entanglement content of any complete set is $\mathcal{E} = 30$. A set of three MU product bases can be constructed from the tensor product of three MU bases of the space $\mathbb{C}^2$ with three MU bases of the space $\mathbb{C}^3$ (see Eq. (3.53)). However, due to the fixed entanglement content, the remaining four bases must contain entangled states only.

2.4.3 A Fourier analytic approach

We now summarise some results from [60] that make use of Fourier analytic arguments in an attempt to simplify the existence problem. Suppose that $\mathcal{G}$ is a compact abelian group and let $\mathcal{A} \subset \mathcal{G}$ be a symmetric subset, called the "forbidden" set, containing the identity element $e \in \mathcal{A}$. The aim is to determine the cardinality of the set $\mathcal{B} = \{b_1 \ldots, b_m\} \subset \mathcal{G}$ such that $b_j - b_k \in \mathcal{A}^c \cup \{e\}$, i.e. the differences $b_j - b_k$ avoid the forbidden set $\mathcal{A}$. Here, $\mathcal{A}^c = \mathcal{G} \setminus \mathcal{A}$ denotes the complement of $\mathcal{A}$.

The solution involves finding a *witness function* $h : \mathcal{G} \to \mathbb{R}$ satisfying the following properties: (i) h is an even function, i.e. $h(x) = h(-x)$, such that the Fourier inversion formula holds for h; (ii) $h(x) \leq 0$ for all $x \in \mathcal{A}^c$; (iii) $\hat{h}(\gamma) \geq 0$ for all $\gamma \in \hat{\mathcal{G}}$; and (iv) $\hat{h}(e) = 1$. Here, $\hat{h}$ and $\hat{\mathcal{G}}$ denote the Fourier transforms of h and $\mathcal{G}$, respectively. A method, given by Delsarte, shows that for a given function h with the above properties, the cardinality of $\mathcal{B}$ is bounded by $|\mathcal{B}| \leq h(e)$.

To relate this problem to MU bases we can choose $\mathcal{G}$ to be the group of $d \times d$ unitary matrices and $\mathcal{A} = H^c$, where $H \subset \mathcal{G}$ is the set of complex Hadamard matrices which have matrix elements of magnitude $1/\sqrt{d}$. One can see that the maximum number of MU bases in $\mathbb{C}^d$ is equivalent to the maximum cardinality of $\mathcal{B} = \{U_0, \ldots, U_m\} \subset \mathcal{G}$, where the differences associated with $U_j^\dagger U_k$ lie in the subset $\mathcal{A}^c \cup I$. However, in this setting, the group $\mathcal{G}$ is not abelian and so the method of Delsarte cannot be directly applied.

To overcome this issue one chooses the group $\mathcal{G} = \mathbb{T}^d$, where $\mathbb{T}$ is the complex unit circle, such that each vector $\vec{v} = (0, \alpha_1, \ldots, \alpha_{d-1}) \in \mathcal{G}$ corresponds to a vector $\vec{v}' = (1, e^{2\pi i \alpha_1}, \ldots, e^{2\pi i \alpha_{d-1}})$ in $\mathbb{C}^d$. Thus, the columns of a set of Hadamard matrices $H_1, \ldots, H_m$ become a set of md vectors denoted by $\vec{v}_i \in \mathbb{T}^d$. Let O_d denote the set of vectors $(0, \alpha_1, \ldots, \alpha_{d-1}) \in \mathbb{T}^d$ which correspond to vectors of $\mathbb{C}^d$ orthogonal to $(1, \ldots, 1) \in \mathbb{C}^d$, and let UB_d denote the set of vectors $(0, \alpha_1, \ldots, \alpha_{d-1}) \in \mathbb{T}^d$ corresponding to vectors of $\mathbb{C}^d$ MU to $(1, \ldots, 1) \in \mathbb{C}^d$. By taking the forbidden set as $\mathcal{A}_d = (O_d \cup UB_d)^c$ we arrive at a scheme for which Delsarte's method applies. As a consequence, we have the following theorem [60]:

Theorem 2.4.3. *Let $\mathcal{A}$ be an orthonormal basis in $\mathbb{C}^d$, and let $\mathcal{B} = \{\vec{c}_1, \ldots, \vec{c}_r\}$ consists of unit vectors which are all unbiased to $\mathcal{A}$. Assume for $1 \leq j \neq k \leq r$ that the vectors $\vec{c}_j$ and $\vec{c}_k$ are either orthogonal or unbiased to each other. Then $r \leq d^2$.*

This result offers an alternative proof that a complete set of MU bases in the space $\mathbb{C}^d$ contains at most $d+1$ bases. The proof of Theorem 2.4.3 involves the construction of a witness function h which takes the form

$$h(0, x_1, x_2, \ldots, x_{d-1}) = \frac{1}{(d-1)d} \left| 1 + \sum_{j=1}^{d-1} e^{2\pi i x_j} \right|^2 \left(|1 - \sum_{j=1}^{d-1} e^{2\pi i x_j}|^2 - d \right). \quad (2.16)$$

The cardinality of $\mathcal{B}$ is bound by the witness function evaluated at $h(0, \ldots, 0) = d^2$. Obviously, no better witness function can be constructed when $d = p^n$. However, when the dimension d is a composite number, it may still be possible to construct a witness function with a lower bound for r. If so, this would prove that complete sets of MU bases only exist in prime-power cases.

Additional work was carried out in [62] making further use of Fourier analysis on the group $\mathcal{G} = \mathbb{T}^d$. In this paper, progress has been made in proving some non-existence results for sets of MU bases, i.e. MU bases that cannot be extended to a complete set. While some of these results are already known, the novelty here is that the proofs do not depend on computer-aided calculations.

To highlight these results it will first be necessary to introduce some further notation in analogy to [62]. The dual group of $\mathcal{G} = \mathbb{T}^d$ is given by $\hat{\mathcal{G}} = \mathbb{Z}^d$, and the action of a character $\gamma = (n_1, n_2, \ldots, n_d) \in \mathbb{Z}^d$ on an element $\vec{v} = (v_1, v_2, \ldots, v_d) \in \mathbb{T}^d$ is given by $\gamma(\vec{v}) = \vec{v}^\gamma = v_1^{n_1} v_2^{n_2} \ldots v_d^{n_d}$. For a set $\mathcal{S} \subset \mathcal{G}$ the Fourier transform is given by $\hat{\mathcal{S}} = \sum_{\vec{s} \in \mathcal{S}} \vec{s}^\gamma$. Thus, given a complete set of MU bases, labelled $I, H_1, \ldots, H_d$, where we consider $H_j \subset \mathcal{G}$ as a d element set $\{\vec{c}_{j1}, \ldots, \vec{c}_{jd}\}$, the Fourier transform of a MU basis is

$$g_j(\gamma) \equiv \hat{H}_j(\gamma) = \sum_{k=1}^{d} \vec{c}_{jk}^{\gamma} \quad \text{for each } \gamma \in \mathbb{Z}^d. \quad (2.17)$$

Two important functions, $F(\gamma)$ and $G(\gamma)$, which prove useful in this framework are given by

$$G(\gamma) \equiv \sum_{j=1}^{d} G_j(\gamma) \quad \text{for each } \gamma \in \mathbb{Z}^d, \tag{2.18}$$

where $G_j(\gamma) \equiv |g_j(\gamma)|^2$ and

$$F(\gamma) \equiv |f(\gamma)|^2, \tag{2.19}$$

where $f(\gamma) \equiv \sum_{j=1}^{d} g_j(\gamma)$ for each $\gamma \in \mathbb{Z}^d$. The orthogonality and unbiasedness relations can then be expressed as *linear* constraints on the functions F and G. In other words, the polynomial relations from the orthogonality and unbiasedness conditions are transformed into linear relations using Fourier transforms, and one should expect that these constraints are simpler to deal with.

The restrictions placed on F and G are enough to derive several known results on MU bases in dimensions $d \leq 5$. It is hoped that a contradiction can be reached from these constraints in cases when complete sets cannot be constructed. The main new result from this approach is the following theorem [62]:

Theorem 2.4.4. *Let $I, H_1, \ldots, H_d$ be a complete system of MU bases, in matrix form, and suppose that H_1 is a real Hadamard matrix. Then there is no further purely real column in any of the matrices $H_2, \ldots, H_d$. In particular it is impossible to have two real Hadamard matrices in a complete set of MU bases.*

In addition, it is also shown that no complete set of MU bases in dimension six contains the pair $\{I, F_6\}$. While this result is already known in [34], and will be discussed in the next section, the original proof uses a computer algebraic approach, whereas the proof provided here relies only on Fourier analytic arguments. Furthermore, a stronger result excluding the existence of a complete set containing the pair $\{I, F_6(a,b)\}$ can be proven using similar arguments *if* the following conjecture is true [62].

Conjecture 2.4.5. *Let H be any complex Hadamard matrix of order 6, not equivalent to the isolated matrix S_6 and let σ be any permutation of the vector* $(1, 1, 1, -1, -1, -1)$*. Then $g_1(\sigma) = 0$ for the function defined in Eq. (2.17).*

A proof of the non-existence of a complete set containing $\{I, F_6(a,b)\}$ is already known, independent of the conjecture's truth [45]. However, the proof relies on a large numerical search using rigorous error bounds which we discuss in more detail in the following section.

It has been predicted that Conjecture 2.4.5 will prove vital in a proof of the non-existence of a complete set in dimension six by offering an additional linear constraint on the function G. By assuming the existence of a hypothetical complete set, a future proof would involve using the linear constraints on F and G to find some structural information on the set of vectors, leading to a contradiction. For example, if in dimension six, $F(\sigma) = 6^4$ for all permutations of $\sigma = (6, -6, 0, 0, 0, 0)$, then one could conclude that the vectors of a complete set in dimension six must consist of sixth roots of unity only. It is easy to check that no such complete set exists. A similar constraint on F exist for dimension four with fourth roots of unity. Unfortunately, the linear constraints involving F and G do not seem to imply the relation $F(\sigma) = 6^4$, and so this particular approach is fruitless.

2.5 Computational results

In this section we review some direct approaches towards solving the existence problem in dimensions six using computational searches. We separate these approaches into numerical results which rely on approximations (numerical analysis) and exact computational calculations which provide rigorous results.

2.5.1 Numerical analysis

The search for MU bases can be recast as an optimisation problem in which one tries to minimise a function that attains a global minimum when a set of orthonormal bases are mutually unbiased. A function of this type was derived in [10] as a measure of distance between orthonormal bases that is maximised if and only if the bases are mutually unbiased. This measure of distance is quite natural when we view the basis vectors of the space $\mathbb{C}^d$ as density matrices in a real $d^2 - 1$ dimensional vector space. In this case, a d dimensional Hilbert space spans a $(d-1)$-plane in a real vector space of dimension d^2-1, and two MU bases correspond to two orthogonal $(d-1)$-planes.

A numerical search involving this minimisation problem was given in [25] for dimension six, and the results suggest that no more than three of the possible seven MU bases exist. The function one attempts to minimise depends on a set of $m \leq d$ orthonormal bases of the space $\mathbb{C}^d$, and is given by

$$f_{d,m}(U_1,\ldots,U_m) = \sum_{0\leq k<l\leq m} \sum_{r,s=1}^{d} \left(\left| \left(U_k^\dagger U_l \right)_{rs} \right|^2 - \frac{1}{d} \right)^2 . \tag{2.20}$$

The m orthonormal bases are represented by $(d \times d)$ unitary matrices $U_1, U_2, \ldots, U_m$, so that the columns within each unitary matrix are orthonormal vectors; the unitary $U_0 \equiv I$ is chosen as the identity matrix. The function achieves a global minimum $f_{d,m} = 0$ if and only if the $m+1$ orthonormal bases are pairwise mutually unbiased, i.e. $|(U_k^\dagger U_l)_{rs}|^2 = 1/d$.

The numerical approach given in [25] searches over all sets of unitaries. Two separate tests to find four and seven unitaries that minimise $f_{d,m}$ were conducted but both failed. The minimum values achieved while searching for four and seven MU bases were $f_{6,3} = 0.051249$ and $f_{6,6} = 1.5844721$, respectively.

Further analysis in [74] reveals a set of four bases that reach the minimum value of $f_{6,3} = 0.051249$ obtained in [25]. In particular, a two-parameter family of orthonormal bases is explicitly found which achieves this minimum for certain parameter values. Of the four bases, three are equidistant and the remaining basis is mutually unbiased to all three. Thus, the set can be written as the identity matrix together with three complex Hadamard matrices. The two-parameter family containing all three Hadamard matrices turns out to be the transposed Fourier family.

Additional numerical searches were explored in [16] focusing on mutually unbiased *constellations*, which were briefly mentioned in Sec. 2.3. Again, this evidence supports the conjecture that only three MU bases exist, and furthermore, that no vector exists which is mutually unbiased to a set of three MU bases. A MU constellation is a set of vectors, partitioned into sets of orthonormal states such that each set of orthonormal states is mutually unbiased to every other set in the constellation. A MU constellation is denoted by $\{x_1, \ldots, x_n\}_d$, where x_i is the number of vectors in a set of orthonormal states, and d is the dimension of the vector space. As an example, the constellation $\{6, 6, 4\}_6$ contains two sets of six orthogonal states, i.e. two MU bases, and a set of four orthogonal states MU to the two bases. We can abbreviate this notation to $\{6^2, 4\}_6$ where 6^2 denotes the two sets of six orthonormal states. In addition, since $d - 1$ orthonormal states determine an orthonormal basis of the space $\mathbb{C}^d$, one can rewrite $\{6^2, 4\}_6$ as the MU constellation $\{5^2, 4\}_6$.

The numerical searches for MU constellations given in [16] use the same minimising technique as [25]. The idea is to rule out the existence of a MU constellation; this, in turn, will imply the inexistence of any set of MU bases for which the MU constellation is a subset. From searches of this type, the largest MU constellations found were $\{5, 4^2, 1\}_6$ and $\{5^2, 3, 1\}_6$, both containing 15 MU states. The smallest MU constellations which the search failed to find were $\{5, 3^3\}_6$ and $\{5, 4, 3, 2\}_6$ with each containing 14 states. The MU constellation $\{5^3, 1\}_6$ containing 16 states was not found, implying the non-existence of a set of three MU bases together with an additional MU state.

Further numerical searches for MU bases were investigated in [10] where a restriction is placed on the vectors such that their components contain only n-th roots of unity. All known complete sets of MU bases satisfy this condition, with their components consisting of either d or $2d$ roots of unity depending on whether the dimension of the Hilbert space d is odd or even, respectively. Thus, in dimension $d = 6$, if a complete set exists, one may reasonably expect its vectors consist of twelfth roots of unity only.

The search over all known complex Hadamard matrices containing only twelfth roots of unity finds at most triples of MU bases. The matrix $F_6(0, 0)$ together with the standard basis has only four possible MU candidate bases. Similarly, $F_6(1/6, 0)$ and $F_6^T(1/6, 0)$ have only one additional candidate basis each. Supplementary searches for 24th, 48th, 60th and 72th roots were carried out, but apart from a further four candidate MU bases for the Diţă-matrix $D_6(1/8)$ [28], no additional bases were found.

Thus, numerical evidence points overwhelmingly towards the non-existence of a complete set of mutually unbiased bases in dimension six. Even the existence of a single vector mutually unbiased to any triple of MU bases is unlikely. If they do exist then it appears they are very well hidden.

2.5.2 Exact results

One of the first results showing that certain sets of MU bases cannot be extended by additional MU bases was given in [34]. Specifically, it is shown that the two MU bases corresponding to the identity and Fourier matrices, I and $F_6(0,0) \equiv F_6$, or equivalently the eigenstates of the Heisenberg-Weyl operators Z and X, do not extend to a complete set of MU bases. In fact, there exist only 48 vectors mutually unbiased to this pair. One can arrange these vectors into 16 different orthonormal bases $\mathcal{B}_i$ to produce 16 MU triples $\{I, F_6, B_i\}$, but there is no vector mutually unbiased to these.

The proof follows by solving a set of polynomial equations. One can express a possible candidate vector of $\mathbb{C}^6$ in the form

$$|\psi\rangle = \frac{1}{\sqrt{6}}(1, x_1 + ix_6, x_2 + ix_7, x_3 + ix_8, x_4 + ix_9, x_5 + ix_{10})^T, \tag{2.21}$$

where the variables x_i are real and $x_i^2 + x_{i+5}^2 = 1$. By requiring that $|\psi\rangle$ is MU to the columns of F_6, and using the computer algebra system MAGMA, one finds 48 real solutions for the set of variables. The 48 vectors are listed explicitly in the updated preprent of [34].

Further analysis of the structure of these 48 vectors, and the corresponding 16 orthonormal bases, has been carried out in [10]. Of the 16 orthonormal bases, two are Fourier matrices enphased with 12th roots of unity, two are equivalent to $F^T(1/6, 0)$, six are Björck matrices [14] and six are Fourier matrices enphased with Björck's number. One interesting feature of any Hadamard matrix which is mutually unbiased to the pair $\{I, F_6\}$ is that it must be *circular*, i.e. $C_{ij} = z_{i-j}$ where $|z_i| = 1$. This is also true in any dimension d for the pair of MU bases $\{I, F_d\}$.

A generalisation of the computer-algebraic calculation given for the Heisenberg-Weyl pair has been made in [17] and includes various other pairs of MU bases $\{I, H_6\}$, where

H_6 is a complex Hadamard matrix. This method relies on the computer program Maple to transform the set of polynomials, using Buchberger's algorithm, to a simpler set, the Gröbner basis, which is easier to solve. All vectors are found which are mutually unbiased to the pair $\{I, H_6\}$, and one subsequently investigates the possible extensions of this pair.

For example, the number of vectors MU to the pairs $\{I, H_6\}$, where H_6 is the Diţă-matrix $D_6(0)$, the circulant matric C_6 [14] and the isolated matrix S_6 is 120, 56 and 90, respectively. While ten triples exist containing the pair $\{I, D_6(0)\}$, none of these extend to four MU bases. Similarly, no four MU bases exist containing $\{I, C_6\}$ and no orthonormal basis can be constructed from the 90 vectors MU to $\{I, S_6\}$.

The same calculation is also carried out at regular intervals over the one-parameter Diţă family $D_6(x)$ and the two-parameter Fourier family $F_6(a, b)$. For the pair $\{I, D_6(x)\}$, the number of MU vectors appears to be piecewise constant, dropping from 120 to 72 and then to 48 at the end points. In the Fourier family $F_6(a, b)$, there exist 48 MU vectors at each of the tested parameter values. In both cases, no set of four MU bases can be constructed.

While these results represent rigorous limits on the number of vectors MU to the pair $\{I, H_6\}$, it is not possible to achieve such rigour when the complex Hadamard matrix H_6 is non-affine. For the symmetric, Hermitian and Szöllősi non-affine families, the available computational memory was insufficient to find the relevant Gröbner basis, thus certain approximations were necessary. While it is unlikely that the approximations fail to identify all of the MU vectors, the result that there exist no four MU bases containing these families is no longer exact.

A subsequent result, presented in [45], has made further progress towards confirming the inexistence of complete sets in dimension six by proving the following.

Theorem 2.5.1. *The family of MU bases $\{I, F_6(a, b)\}$ cannot be extended to a quartet of MU bases.*

Previously, this result was only known for a finite subset of the two-parameter family $F_6(a, b)$, as discussed above. The proof of Theorem 2.5.1 relies on a discretisation scheme and a computational search similar to [16], but the result here is rigorous by establishing proper estimates of the error terms. The search for candidate MU vectors involves finding approximate MU vectors by estimating the phases of the vector components using N-th roots of unity. Each vector component is evaluated at regular intervals of $2\pi j/N$, with $j = 1, \ldots, N$, and a computer-aided search calculates N^{ν} states, where ν denotes the number of free variables (phases) for the candidate MU vectors. By choosing a sufficiently large positive integer N, rigorous bounds of the errors, given by the inner products of the approximated states, can be established. If the errors from these approximated states are too large, no such MU vectors exist. Importantly, this method can be generalised and could, theoretically, constitute a proof of the inexistence of complete sets in dimension six, even without a classification of (6×6) complex Hadamard matrices [44].

The computational search over the parameter values (a, b) reveals the number of vectors MU to the pair $\{I, F_6(a, b)\}$ to be 48, confirming the findings of [16]. In most cases these 48 vectors produce 8 orthonormal bases $C_1(a, b), \ldots, C_8(a, b)$. In exceptional cases one can construct additional orthonormal bases, e.g. for $(a, b) = (0, 0)$ and $(a, b) = (1/6, 0)$, there exist 16 and 70 orthonormal bases, respectively.

It is also shown in [45] that a one-parameter family of triples $\{I, F_6(0, b(t)), C(t)\}$ exists, which is found in closed analytic form. This complements an infinite family of triples found in [98] which is written explicitly in [45]. In addition, the numerical calculations which find 48 vectors MU to $\{I, F_6(a, b)\}$ point to the existence of a two-parameter family of MU triples, but this has not been proven rigorously.

Another possible computational approach to rule out, rigorously, the existence of certain MU bases is semi-definite programming [18]. This technique involves an optimisation problem for the set of polynomials $p_i(\vec{x})$ that provides the constraints for the MU basis vectors; the real variables $\vec{x} = (x_1, \ldots, x_n)$ parameterise the possible candidate vectors. The general idea is to minimise one polynomial, $p_k(\vec{x})$, subject to the condition $p_i(\vec{x}) = 0$ for all $i \neq k$. If a positive global bound is found for this minimisation, no solution and therefore no set of MU bases exists. This method confirms the non-existence of a

MU triple containing the pair $\{I, S_6\}$, where S_6 is the isolated Hadamard matrix, but it is unsuccessful for the constellation $\{5^3, 1\}$ due to the increase in computational complexity [18].

2.6 Applications of MU bases

We now summarise some of the popular applications of MU bases in the field of quantum information. These include quantum state tomography, quantum key distribution and the King's problem. While we find that MU bases are an important ingredient for these applications, it is not vital that *complete* sets of MU bases exist. However, this in no way diminishes the interesting mathematical and physical questions that arise from their probable inexistence.

2.6.1 State tomography

One of the most striking applications of MU bases is revealed in the problem of quantum state determination (quantum tomography). In fact, complete sets of MU bases for prime and prime-power dimensions were first discovered in a solution to the problem of optimal quantum state determination. MU measurements play a key role in optimising the information gain, or minimising the statistical error, for estimating a given quantum state [43, 97].

In the process of state estimation it is first assumed that we have a large but finite ensemble of identical d-state systems. The aim is to determine the density matrix $\rho \in \mathcal{S}(\mathcal{H})$ of the system, where $\mathcal{S}(\mathcal{H})$ is the set of positive trace class operators of trace one. The ensemble is divided into $d + 1$ subensembles, each of equal size, and on each subensemble we perform a different measurement. From the outcome probabilities of these measurements we can reconstruct the pre-measurement state ρ.

The measurements we choose, as long as they are informationally complete, will give an estimate of the state ρ with some degree of statistical error. By choosing $d + 1$ measurements which are pairwise complementary, the statistical error is minimised [97].

In this case, the r-th measurement is given by a set of orthogonal projection operators $\{P_i^{(r)}\}$, $i = 1, \ldots, d$, which project the measured state onto the eigenvectors of an orthonormal basis, mutually unbiased to the remaining d measurements.

For the simplest case, $d = 2$, the density matrix to find is $\rho = \frac{1}{2}(I + \vec{r}.\vec{\sigma})$, with I the identity matrix and $|\vec{r}| \leq 1$. The complementary spin observables σ_x, σ_y and σ_z are then measured on separate subensembles, with each spin direction producing one component of $\vec{r}$, and the state is unambiguously determined. Since every measurement has some degree of statistical inaccuracy, each measurement confines $\vec{r}$ to a plane which is a "fuzzy" estimate of the exact plane. The intersection of the three "fuzzy" planes represents the inaccuracy in the measurement of $\vec{r}$. The error is minimised if the planes are mutually perpendicular, i.e. the measurements are mutually unbiased, as one would intuitively expect.

If a complete set of $d + 1$ MU measurements do not exist, all subspaces cannot be pairwise orthogonal and the problem of state optimisation becomes somewhat more complicated. Without knowledge of a complete set, or even if no such set exist, can we still find an optimal reconstruction procedure for the state in question? Fortunately, a successful alternative to the MU approach to state reconstruction has been found for arbitrary dimensions. Thus, it appears that the existence of complete sets in arbitrary dimensions – while an important ingredient – is not fundamental for optimal quantum tomography.

In the generalisation to arbitrary d-level systems, weighted complex projective 2-designs now play the important role in optimising the state reconstruction [76]. These particular 2-designs are generalisations of complete sets of MU bases; in fact a complete set of $d+1$ MU bases is an example of a complex projective 2-design [52]. It has been shown that the set of bases which constitute a weighted 2-design form the orthogonal measurements necessary for optimal quantum tomography [76].

To define a 2-design let $f(x)$ be a homogenous polynomial of degree 2 on $\mathbb{C}^d$ evaluated over its coordinates and their complex conjugates (with respect to some fixed basis), i.e. $f(x) = f(x_1, \ldots x_d, x_1^*, \ldots, x_d^*)$, and denote the set of these polynomials by $\mathrm{Hom}(2, 2)$.

Then a *weighted complex projective* 2*-design* is a set of normalised vectors $\mathcal{D}$ in $\mathbb{C}^d$, with a normalised weight function $w : \mathcal{D} \to [0,1]$, such that for all $f \in \text{Hom}(2,2)$ the relation

$$\sum_{x\in\mathcal{D}} w(x) f(x) = \int_{\mathbb{C}P^{d-1}} f(x) dx \tag{2.22}$$

holds. Here, dx denotes the Haar measure on the complex projective space $\mathbb{C}P^{d-1}$.

Explicit examples of weighted 2-designs are constructed in [76] for $d+1$ a prime-power where a set of $d+2$ orthonormal bases is found. This covers dimension six, in which eight orthonormal bases form a weighted 2-design. Here, starting with the standard basis $\{|e_0\rangle, \ldots, |e_5\rangle\}$, the remaining seven orthonormal bases are given by

$$|e_j^a\rangle = \frac{1}{\sqrt{6}} \sum_{k=0}^{5} \omega^{jk} e^{2\pi i a 3^k/7} |e_k\rangle, \tag{2.23}$$

where $a = 1, \ldots, 7$ and $\omega = e^{2\pi i/6}$. The overlap between elements of different bases, given explicitly in [69], is

$$|\langle e_i^a | e_j^b \rangle|^2 = \begin{cases} \frac{6}{7} & \text{if } a \neq b,\ i \neq j\,, \\ \frac{1}{36} & \text{if } a \neq b,\ i = j\,. \end{cases} \tag{2.24}$$

Surprisingly, by performing the measurements associated with the eight orthonormal bases on the unknown quantum state – the standard basis is measured in the ratio 7 : 6 with respect to each of the remaining bases – optimal state reconstruction can be achieved. In fact, the same statistical error is minimised as would be the case if a complete set of seven MU bases existed.

In higher composite dimensions, when $d+1$ is not prime, the minimum number of orthonormal bases needed to construct a weighted 2-design for optimal state reconstruction is not known explicitly, but an upper bound is given in [76]. This bound was improved in [64] where weighted 2-designs are found to contain roughly $2(d+\sqrt{d})$ bases when d is odd and $3(d+\sqrt{d})$ for d even.

Another approach to quantum state reconstruction of an arbitrary d-level system is to recast the problem in terms of special types of informationally complete positive operator value measures (IC-POVM). These are called *tight* rank-one IC-POVMs [81] and are *equivalent* to complex projective 2-designs. Both SIC-POVMs and complete sets of MU bases are examples of tight rank-one IC-POVMs. It is shown in [81] that tight rank-one IC-POVMs are optimal for *linear* quantum state tomography. The state reconstruction is "linear" in the sense that it is limited to a simplified state reconstruction procedure.

2.6.2 Quantum key distribution

The process of measurement in quantum systems in some way disturbs the state of the system. This fundamental aspect of quantum mechanics has been the springboard to applications in quantum cryptography. In particular, one can share a *secret key*, which can be used to encrypt a message between two parties such that it is impossible for some outside entity to gain information of the key without disturbing its content and being detected.

The first example of quantum key distribution was discovered in [11] and it is often referred to as the BB84 protocol. A secret key, usually some *random* assortment of bits, e.g. 010110, is sent via a series of qubit states to a receiver. The states belong to two orthonormal bases, $\mathcal{B}_z = \{|0\rangle, |1\rangle\}$ and $\mathcal{B}_x = \{|+\rangle, |-\rangle\}$, corresponding to the spin operators σ_z and σ_x, respectively. Within each basis, each state represents one of the two bits 0 and 1. The sender chooses the basis *randomly*, and the appropriate state corresponding to 0 or 1. The state is transmitted using a secure quantum channel to the receiver, who then measures the state using either σ_z or σ_x, chosen randomly. If the receiver chooses the correct measurement, which will occur in half of all cases, the correct state can be determined accurately.

After the measurements are made, the basis and measurement choices are revealed through some public communication channel. When the sender and receiver have made different basis choices, the associated bits are removed from the key. To check security they compare a subset of their key and if errors appear, a breach must have occurred. If the error rate is below a certain bound, it is possible to delete the incorrect bits and to reduce the knowledge gained by the eavesdropper.

Other quantum key distribution protocols have since been developed and successful implementation for various schemes has been achieved experimentally and commercially [79]. The optimal or most robust protocol is one which can tolerate large disturbances (errors) and still result in secure key distribution. This depends on the eavesdropper's strategy and so considerable effort is invested towards finding the optimal method of attack for each protocol. The optimal eavesdropping strategy for the BB84 protocol is known for *individual* attacks [26], and when unlimited resources are available to the eavesdropper, the protocol is secure.

In the BB84 protocol, only two mutually unbiased bases are used. A variation of this is a six-state protocol where an additional MU basis is considered. A further generalisation was made in [26] to d-level systems using either two MU bases in $\mathbb{C}^d$, or a complete set of $d+1$ MU bases, when they exist. If individual attacks are considered by means of a quantum cloning machine, a slightly higher error rate is achieved with a set of $d+1$ MU bases compared to just two, however, practically it is the two basis protocol which is preferred since a longer key can be produced.

2.6.3 The King's problem

Another slightly less natural application of MU bases is their role in the solution to a measurement problem involving a fictitious "mean" King. The problem evolved from a scenario whereby an observer A prepares a spin-$\frac{1}{2}$ particle in a state of her choice and then performs a control measurement on the system. Between the preparation and measurement, a second observer B measures either σ_x, σ_y or σ_z on the particle state. After the control measurement, observer A is told which spin component observer B measured and is asked to determine the corresponding measurement outcome [90].

The generalisation of this problem is usually told by the following story: a King who lives on a remote island sets a physicist a life or death challenge. He asks the physicist to prepare an d-state quantum system of her choice and to perform a control measurement on the system. Before her control measurement, she must hand the state over to the King while he secretely performs a measurement. After her control measurement the

King reveals his measurement and challenges her to determine the outcome. In this generalisation, the choice of measurement made by the King is restricted to pairwise complementary observables.

The generalised problem was first solved for a system with prime degrees of freedom in [32] and then extended to include prime-powers [3]. Crucially, both solutions rely on the existence of complete sets of MU bases. To solve this, the physicist prepares two d-state systems in a maximally entangled state of the space $\mathbb{C}^d \otimes \mathbb{C}^d$. The auxiliary system is kept by the physicist while the King preforms one of $d+1$ mutually unbiased measurements on the object system.

Under these assumptions, and by restricting the measurement made by the physicist to a projection-valued measure (PVM), the King's problem for an arbitrary d-state system has a solution only if the maximum number of $d-1$ mutually orthogonal (MO) Latin squares exist [37]. If d is a prime or prime-power, this maximum is achieved and the solutions agree with those given in [3,32]. However, in dimension $d = 6$ only three MO Latin squares exist, implying that there is no solution to the problem for this degree of freedom, regardless of whether a complete set of seven MU bases exist. Similarly, this is true for $d = 10$ since no set of nine MO Latin squares exist.

By extending the type of measurement made by the physicist on the space $\mathbb{C}^d \otimes \mathbb{C}^d$ to include POVM measurements, a full solution to the King's problem has now been found for arbitrary levels [50]. Thus, regardless of whether $d-1$ MO Latin squares or complete sets of MU bases exist, the physicist can always determine the King's measurement outcome.

Chapter 3

All MU product bases in dimension 6

In this chapter we carry out a comprehensive study of MU product bases in dimensions six, complementing studies devoted to the entanglement structure of *complete* sets of MU bases [58, 75, 93]. More specifically, we will derive an exhaustive list of MU product bases in dimension six. The restriction to product states goes hand in hand with local equivalence transformations, or LETs, consisting of *local* (anti-) unitary transformations. We will find that in the space $\mathbb{C}^2 \otimes \mathbb{C}^3$, there is a considerable number of inequivalent product bases, a limited set of families of MU product *pairs* and just two *triples* of MU product bases. No larger MU product constellations exist. This result effectively limits the number of MU product bases contained in a hypothetical complete set of MU bases in dimension six.

The argument will unfold as follows. In Sec. 3.1 we introduce MU product bases, specify all local (anti-) unitary transformations which map a given set of MU product states to an equivalent one, and summarise relevant properties of MU bases in dimensions two and three. Then, in Sec. 3.2, we derive all inequivalent product bases in $\mathbb{C}^4$ and $\mathbb{C}^6$. Sec. 3.3 has two results on product vectors required to be MU to certain given sets of MU product vectors. These results will be important tools to enumerate all pairs and triples of MU bases in dimension four (Sec. 3.4) and dimension six (Sec. 3.5). This classification allows us to conclude, as shown in Sec. 3.6, that no MU product triple can be part of a complete set of seven MU bases in $d = 6$. The final section summarises our findings.

Readers mainly interested in the results relevant to dimension six are advised to immediately proceed to Sec. 3.5 after having familiarised themselves with the concept of mutually unbiased product bases presented in Sec. 3.1.

3.1 MU product bases

From now on, we will consider quantum systems consisting of two subsystems with prime dimensions p and q, where $p \leq q$. The state space of such a bipartite system is given by the Hilbert space $\mathbb{C}^p \otimes \mathbb{C}^q$ of dimension $d \equiv pq$. Since p is a prime, there is a complete set of $(p+1)$ MU bases for $\mathbb{C}^p$ labelled by the states

$$|j_a\rangle \in \mathbb{C}^p\,, \quad j = 0 \ldots p-1,\, a = 0 \ldots p\,, \tag{3.1}$$

which satisfy the condition

$$|\langle j_a|k_b\rangle|^2 = \frac{1}{p}(1-\delta_{ab}) + \delta_{jk}\delta_{ab}, \quad j,k = 0 \ldots p-1,\, a,b = 0 \ldots p\,. \tag{3.2}$$

The p states $\{|j_a\rangle\}$ form one orthonormal basis labelled by a and states taken from two distinct bases are mutually unbiased. Similarly, there is a complete set of MU bases of $\mathbb{C}^q$, and we will denote its $q(q+1)$ states by

$$|J_b\rangle \in \mathbb{C}^q\,, \quad J = 0 \ldots q-1,\, b = 0 \ldots q\,. \tag{3.3}$$

The q states $\{|J_b\rangle\}$ form an orthonormal basis labelled by b and every pair of bases is MU, in analogy to Eq (3.2). Given complete sets of MU bases in $\mathbb{C}^p$ and $\mathbb{C}^q$, respectively, we now construct $(p+1)$ MU *product* bases of the space $\mathbb{C}^p \otimes \mathbb{C}^q$. To do so, we pair each MU basis of the space $\mathbb{C}^p$ with a (different) basis of $\mathbb{C}^q$ and, within each pair, we tensor each state of the first basis with a (different) state of the second one. This procedure results in $pq(p+1)$ *product* states

$$|j_a\rangle \otimes |J_a\rangle \equiv |j_a, J_a\rangle\,, \tag{3.4}$$

forming $(p+1)$ MU bases $\{|j_a, J_a\rangle, a = 0 \ldots p\}$ of the space $\mathbb{C}^p \otimes \mathbb{C}^q$. This is evident upon calculating the overlaps

$$|\langle j_a, J_a|k_b, K_b\rangle|^2 = |\langle j_a|k_b\rangle|^2 \, |\langle J_a|K_b\rangle|^2 = \begin{cases} \delta_{jk}\delta_{JK} & \text{if } a = b\,, \\ \frac{1}{pq} & \text{if } a \neq b\,, \end{cases} \tag{3.5}$$

which are the conditions for bases to be MU in a space of dimension pq.

One can construct MU product bases of the type given in Eq. (3.4) using Heisenberg-Weyl (HW) operators. In dimension p, with p prime, the HW cyclic shift (modulo p) and phase operators X_p and Z_p, respectively, are defined in analogy to Eq. (2.12).

For the composite dimension $d = pq$, we can build a set of $(p+1)$ MU product bases of the Hilbert space $\mathbb{C}^p \otimes \mathbb{C}^q$ with the operators X_p and Z_p acting on the space $\mathbb{C}^p$, and X_q and Z_q on the space $\mathbb{C}^q$. For example, the eigenbases of the operators $X_p \otimes X_q$ and $Z_p \otimes Z_q$ form two MU product bases, which we call a Heisenberg-Weyl pair. One can also construct HW bases with the operators X_{pq} and Z_{pq} on the space $\mathbb{C}^{pq}$, however, these do not necessarily form product bases. Since we are concerned with product bases in this paper, we define the HW operators on the space $\mathbb{C}^p \otimes \mathbb{C}^q$ such that their eigenstates are product states. Note that we do not limit the construction of MU bases to the eigenbases of HW operators, i.e. $\{|j_a, J_a\rangle\}$ in (3.4) can be *any* product basis.

Each basis $\{|j_a, J_a\rangle\}$ is a *direct* product basis of the space $\mathbb{C}^p \otimes \mathbb{C}^q$ since *each* state $|j_a\rangle, j = 0 \ldots p-1$, of the a^{th} basis in $\mathbb{C}^p$ is multiplied with *every* state $|J_a\rangle, J = 0 \ldots q-1$, of the a^{th} basis of $\mathbb{C}^q$. Direct product bases are, however, only a subset among all product bases: *indirect* product bases [93] result if the states being tensored stem from more than one basis of the space $\mathbb{C}^p$ (or $\mathbb{C}^q$). The four states

$$\{|0_z, 0_z\rangle, |0_z, 1_z\rangle, |1_z, 0_x\rangle, |1_z, 1_x\rangle\} \tag{3.6}$$

provide a simple example of an *indirect* product basis in dimension four since two different bases of the second space, $\{|j_z\rangle\}$ and $\{|j_x\rangle\}$, occur in the construction. The matrix representation of a *direct* product basis in dimension $d = pq$ is given by the tensor product of two matrices, each representing a basis of the spaces $\mathbb{C}^p$ and $\mathbb{C}^q$, respectively. The matrix representation of an *indirect* product basis cannot be written as a tensor product of two matrices.

Conceptually, the distinction between direct and indirect product bases is not linked to MU bases: instead of using $\{|j_z\rangle\}$ and $\{|j_x\rangle\}$ in (3.6) any other pair of bases of $\mathbb{C}^2$ would also define an indirect product basis. Indirect product bases are important since they have been found to exhibit a degree of non-locality in the absence of entanglement [12].

In this chapter we will be concerned exclusively with product bases of the spaces $\mathbb{C}^2 \otimes \mathbb{C}^2$ and $\mathbb{C}^2 \otimes \mathbb{C}^3$. To simplify the construction of all different MU product bases, we will now introduce equivalence relations which respect the structure of product states, followed by a brief reminder of the properties of MU bases in $\mathbb{C}^2$ and $\mathbb{C}^3$ following conventions used in [18].

3.1.1 Local equivalence transformations

Given a set of MU bases on the space $\mathbb{C}^p$, we obtain another set by applying one single unitary transformation to all states simultaneously. The scalar products between the states of the MU bases do not change under this transformation so that we deal indeed with a second set of MU bases, factually *different* from the initial set but *equivalent* to it. By not distinguishing between equivalent MU bases, their enumeration is greatly simplified. When representing MU bases by Hadamard matrices, the concept of a standard (or dephased) form emerges naturally (see [10], for example). To enumerate all MU *product* bases it will be helpful not to distinguish those sets of MU product bases which can be transformed into each other by *local* equivalence transformations, or LETs, for short. LETs are defined by the requirement that they preserve the product structure of all states. If there is no LET transforming two given sets of MU product states into each other they will be called *locally inequivalent*, or just *inequivalent.* It may still be possible to transform them into each other by *non-local* transformations.

We now list all LETs for a bipartite quantum system with Hilbert space $\mathbb{C}^p \otimes \mathbb{C}^q$. Suppose we are given sets of $(r+1)$ MU bases $\{\mathcal{B}_0, \mathcal{B}_1, \ldots, \mathcal{B}_r\}$ that contain only product states. Explicitly, the ρ^{th} basis, with $\rho = 0 \ldots r$, consists of $d = pq$ product states $|n_\rho, N_\rho\rangle$, $n \equiv N \in \{1, 2, \ldots, d\}$, where $|n_\rho\rangle \in \mathbb{C}^p$ and $|N_\rho\rangle \in \mathbb{C}^q$. Any combination of the following five operations maps the given set of MU bases into a locally equivalent set:

1. a *local unitary* transformation $\hat{u} \otimes \hat{U}$ effecting
$$\mathcal{B}_\rho \to \mathcal{B}'_\rho = \hat{u} \otimes \hat{U} \mathcal{B}_\rho \equiv \Big\{ \ldots, |\hat{u} n_\rho\rangle \otimes |\hat{U} N_\rho\rangle, \ldots \Big\}, \tag{3.7}$$
which leaves invariant the value of all scalar products;

2. the multiplication of all states within a basis by possibly different *phase factors* such that
$$\mathcal{B}_\rho \to \mathcal{B}'_\rho = \Big\{ \ldots, e^{i\phi_n^\rho} |n_\rho, N_\rho\rangle, \ldots \Big\}; \tag{3.8}$$
these transformations exploit the fact that the overall phase of a quantum state has no physical significance and automatically drops out from the conditions defining MU bases. It is worth noting that a single phase factor $e^{i\phi}$ can dephase *both* states of a product: let $\phi \equiv \phi' + \phi''$ to find $e^{i\phi}|n_\rho, N_\rho\rangle = (e^{i\phi'}|n_\rho\rangle) \otimes (e^{i\phi''}|N_\rho\rangle)$;

3. *permutations* of the product states within each basis; as an example, consider the permutation of states $|n_\rho, N_\rho\rangle$ and $|n'_\rho, N'_\rho\rangle$ in the ρ^{th} basis
$$\Big\{ \ldots, |n_\rho, N_\rho\rangle, \ldots, |n'_\rho, N'_\rho\rangle, \ldots \Big\} \longrightarrow \Big\{ \ldots, |n'_\rho, N'_\rho\rangle, \ldots, |n_\rho, N_\rho\rangle, \ldots \Big\}, \tag{3.9}$$
which amounts to relabelling the elements within each basis;

4. the *local complex conjugations* $\hat{k} \otimes \hat{I}$ and $\hat{I} \otimes \hat{K}$ (anti-unitary operations defined with respect to the standard bases in $\mathbb{C}^p$ and $\mathbb{C}^q$, respectively), and thus their product $\hat{k} \otimes \hat{K}$; for example, applying $\hat{k} \otimes \hat{I}$
$$\mathcal{B}_\rho \to \mathcal{B}'_\rho = \Big\{ \ldots, |n^*_\rho, N_\rho\rangle, \ldots \Big\}, \tag{3.10}$$
swaps all scalar products resulting from the first factors without changing their numerical values;

5. *pairwise exchanges* of two bases, which amounts to relabelling the bases.

We now briefly discuss some important properties of LETs. First, they represent a true subset of all equivalence transformations in a space of dimension pq: no LET maps an indirect product basis to a direct one while a general unitary equivalence transformation can send any orthonormal basis to any other. Second, we will find indirect product bases which cannot be transformed into each other by LETs, i.e. *locally inequivalent* product bases. As a result, the idea of a *unique* standard or dephased form of MU bases is less straightforward for MU product bases. We define a standard form in the following way: the first basis $\mathcal{B}_0$, be it direct or indirect, contains the states $\{|j_z\rangle\}$ of the space $\mathbb{C}^p$ and the states $\{|J_z\rangle\}$ of the space $\mathbb{C}^q$; the second basis $\mathcal{B}_1$ contains the state $|0_x, 0_x\rangle$, and all other states in the remaining bases are dephased using the transformation defined in (3.8). Superficially, LETs remind one of local operations with classical communication, or LOCCs [67]. However, the presence of anti-unitary operations rather suggests a link with Wigner's theorem about symmetry transformations leaving transition probabilities invariant [94], for the special case of a universe populated with product states only. Finally, it is straightforward to generalise LETs to n-partite systems residing in product states only.

It is often convenient to represent an MU product basis in $\mathbb{C}^{pq}$ as a complex Hadamard matrix of dimension $(pq \times pq)$, with each product state corresponding to one column. The bases $\{\mathcal{B}_0, \mathcal{B}_1, \ldots, \mathcal{B}_r\}$ then turn into a set of $(r+1)$ matrices, on which the five transformations above act in the following way. The first LET is a *local unitary*, given by the Kronecker product of two unitary matrices, applied to all matrices from the left; the second LET corresponds to *diagonal unitary* transformations acting from the right; *unitary permutation matrices* acting from the right implement the third type of LET, while the effect of the *local complex conjugations* must be worked out by writing down each product state individually.

3.1.2 MU bases in dimensions two and three

Given a pair of MU bases in the vector space $\mathbb{C}^2$, we can always map the first basis to the standard basis $\{|j_z\rangle\}$ by a suitable unitary transformation $\hat{u} \in SU(2)$. Being MU to the first basis, the states of the second basis now must have the form

$$|a\rangle = \frac{1}{\sqrt{2}}(|0_z\rangle + e^{i\lambda}|1_z\rangle) \equiv \hat{r}_\lambda|+\rangle \, , \quad |a^\perp\rangle = \hat{r}_\lambda|-\rangle \, , \tag{3.11}$$

where $\{|\pm\rangle\} \equiv \{|j_x\rangle\}$ is the x-eigenbasis, and the operator $\hat{r}_\lambda, \lambda \in [0,\pi)$, represents a rotation by an angle λ about the z-axis. Since any such rotation leaves the standard basis $\{|j_z\rangle\}$ unchanged, the second MU basis can be transformed into $\{|j_x\rangle\}$. The matrix representation of the resulting pair of MU bases reads

$$\{I; F_2\} \equiv \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} ; \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \right\} . \tag{3.12}$$

All other pairs of MU bases of the space $\mathbb{C}^2$ are, in fact, equivalent to this one. A third basis MU to these two bases consists of the states given in Eq. (3.11) if $\lambda = \pm\pi/2$, producing $\{|j_y\rangle\}$. Thus, all pairs of MU bases in $\mathbb{C}^2$ are equivalent to $\{|j_z\rangle; |j_x\rangle\}$, and all triples are equivalent to $\{|j_z\rangle; |j_x\rangle; |j_y\rangle\}$, as is well known.

In dimension three, one of two given MU bases can always be mapped to the standard basis $\{|J_z\rangle, J = 0,1,2\}$, so that the second basis consists of states of the form

$$|A\rangle = \frac{1}{\sqrt{3}}(|0_z\rangle + e^{i\xi}|1_z\rangle + e^{i\eta}|2_z\rangle) , \quad \xi, \eta \in [0, 2\pi) , \tag{3.13}$$

exploiting the fact that the overall phase of a quantum state has no physical meaning. One can construct three states of this form which are pairwise orthogonal: writing

$$|A^\perp\rangle = \frac{1}{\sqrt{3}}(|0_z\rangle + \gamma e^{i\xi}|1_z\rangle + \delta e^{i\eta}|2_z\rangle) , \quad |\gamma| = |\delta| = 1 , \tag{3.14}$$

the condition $\langle A|A^\perp\rangle = 0$ implies $\gamma + \delta = -1$. A geometric argument in the complex plane implies either $\gamma = \omega$ and $\delta = \omega^2$, or $\gamma = \omega^2$ and $\delta = \omega$, where $\omega = e^{2\pi i/3}$ is a third root of unity. We denote the resulting basis by

$$\{|A\rangle, |A^\perp\rangle, |A^{\perp\!\perp}\rangle\} = \{\hat{R}_{\xi,\eta}|J_x\rangle\} , \tag{3.15}$$

where the triple $\{|J_x\rangle\} \equiv \{|J_x\rangle, J = 0,1,2\}$ consists of the eigenstates of the shift operator $\hat{X}_3$, and the operator $\hat{R}_{\xi,\eta}$ is diagonal in the z-basis such that $|A\rangle \equiv \hat{R}_{\xi,\eta}|0_x\rangle$, cf. Eq. (3.13). The free parameters ξ, η in the pairs of MU bases $\{|J_z\rangle; \hat{R}_{\xi,\eta}|J_x\rangle\}$ can be removed by a suitable redefinition of the phases of the states in the standard basis $\{|J_z\rangle\}$. Thus, all pairs of MU bases of $\mathbb{C}^3$ are equivalent to the pair $\{|J_z\rangle; |J_x\rangle\}$ which may be represented by

$$\{I;F_3\} = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} ; \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \right\} , \tag{3.16}$$

where $F_3 \equiv H_x$ is the Fourier matrix in $\mathbb{C}^3$. Note that two more orthonormal bases of states MU to the pair $\{|J_z\rangle; |J_x\rangle\}$ emerge if one sets either $e^{i\xi} = e^{i\eta} \equiv \omega$ or $e^{i\xi} = e^{i\eta} \equiv \omega^2$ in Eq. (3.15). We will denote these bases by $\{|J_y\rangle\}$ and $\{|J_w\rangle\}$, respectively, and their matrix representations are given by

$$H_y = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ \omega & \omega^2 & 1 \\ \omega & 1 & \omega^2 \end{pmatrix} , \quad H_w = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ \omega^2 & 1 & \omega \\ \omega^2 & \omega & 1 \end{pmatrix} , \tag{3.17}$$

which are also MU with respect to each other. The matrices H_x, H_y and H_w are complex (3×3) Hadamard matrices, i.e. they are unitary and the moduli of all their entries are equal to $1/\sqrt{3}$.

Two *triples* of MU bases now result from adding either $\{|J_y\rangle\}$ or $\{|J_w\rangle\}$ to the pair $\{|J_z\rangle; |J_x\rangle\}$. These triples are equivalent to each other as follows from taking the complex conjugate (defined in the z-basis) of the triple $\{|J_z\rangle; |J_x\rangle; |J_y\rangle\}$: the complex conjugation only affects the ordering of states within $\{|J_x\rangle\}$ while $\{|J_y\rangle\}$ turns into $\{|J_w\rangle\}$. Thus we conclude that the triples are indeed equivalent which we express formally by writing

$$\{|J_z\rangle; |J_x\rangle; |J_y\rangle\} \sim \{|J_z\rangle; |J_x\rangle; |J_w\rangle\} . \tag{3.18}$$

Consequently, all MU triples are equivalent to the triple $\{|J_z\rangle; |J_x\rangle; |J_y\rangle\}$, and the complete set of four MU bases in $\mathbb{C}^3$ is also unique, as is well known.

3.2 Constructing product bases in dimensions four and six

The first step towards an exhaustive list of pairs and triples of MU product bases in dimension six is to construct all locally inequivalent product bases in $\mathbb{C}^2 \otimes \mathbb{C}^3$. Once these are known, the requirement of any two such bases to be MU will impose further constraints. It will be helpful to initially carry out this construction in dimension four. Thus, we will first derive all inequivalent product bases of the space $\mathbb{C}^2 \otimes \mathbb{C}^2$, followed by a similar construction for a six-dimensional space.

3.2.1 All product bases in $d = 4$

We now show that each product basis in $d = 4$ is equivalent either to the standard *direct* product basis or to a member of two families of *indirect* product bases, each depending on two real parameters. Any (orthonormal) product basis in the space $\mathbb{C}^2 \otimes \mathbb{C}^2$ must have the form

$$\Big\{|\psi_1, \phi_1\rangle,\, |\psi_2, \phi_2\rangle,\, |\psi_3, \phi_3\rangle,\, |\psi_4, \phi_4\rangle\Big\}\,, \tag{3.19}$$

where $|\psi_n\rangle, |\phi_n\rangle \in \mathbb{C}^2$ for $n = 1 \ldots 4$. The conditions

$$\langle\psi_n, \phi_n|\psi_{n'}, \phi_{n'}\rangle = \langle\psi_n|\psi_{n'}\rangle\langle\phi_n|\phi_{n'}\rangle = \delta_{nn'}\,, \quad n, n' = 1 \ldots 4\,, \tag{3.20}$$

imply that at least two states of the first factor must be orthogonal: assume that there is no orthogonal pair among the states $|\psi_1\rangle$, $|\psi_2\rangle$ and $|\psi_3\rangle$; then, the states $|\phi_1\rangle, |\phi_2\rangle$ and $|\phi_3\rangle$ must be pairwise orthogonal. However, no three orthogonal states exist in $\mathbb{C}^2$, so that upon calling $|\psi_1\rangle \equiv |a\rangle$ we must have

$$\Big\{|a, \phi_1\rangle,\, |a^\perp, \phi_2\rangle,\, |\psi_3, \phi_3\rangle,\, |\psi_4, \phi_4\rangle\Big\}\,, \tag{3.21}$$

with $|\psi_2\rangle = |a^\perp\rangle$ being the unique state (up to a phase factor) orthogonal to $|a\rangle$. Now we need to consider two separate cases: we can have either $|\psi_3\rangle = |a\rangle$ (or, equivalently, $|\psi_3\rangle = |a^\perp\rangle$) or $|\psi_3\rangle = |b\rangle$ such that $0 < |\langle a|b\rangle| < 1$, meaning that the state $|b\rangle$ is neither a multiple of the state $|a\rangle$ nor orthogonal to it; we call such a vector $|b\rangle$ *skew* to $|a\rangle$.

Case 1: If $|\psi_3\rangle = |a\rangle$, then the states $|\phi_1\rangle$ and $|\phi_3\rangle$ must be orthogonal. This implies that the state $|\psi_4\rangle$ must be orthogonal to $|a\rangle$ – if it was not, $|\phi_4\rangle$ would have to be orthogonal to the orthogonal pair $|\phi_1\rangle$, $|\phi_3\rangle$, which is impossible. Thus, we find

$$\Big\{|a, A\rangle,\, |a^\perp, \phi_2\rangle,\, |a, A^\perp\rangle,\, |a^\perp, \phi_4\rangle\Big\}\,, \tag{3.22}$$

where we write $|A\rangle$ to denote $|\phi_1\rangle$. Finally, the condition $\langle\phi_2|\phi_4\rangle = 0$ restricts the states involved to be *any* orthonormal pair, $|\phi_2\rangle = |B\rangle$, and $|\phi_4\rangle = |B^\perp\rangle$, say. Two qualitatively different cases result depending on whether we have $|B\rangle \equiv |A\rangle$,

$$\mathcal{B}_0 = \Big\{|a, A\rangle, \, |a, A^\perp\rangle, \, |a^\perp, A\rangle, \, |a^\perp, A^\perp\rangle\Big\} \tag{3.23}$$

or $|B\rangle$ being skew to $|A\rangle$,

$$\mathcal{B}_1 = \Big\{|a, A\rangle, \, |a, A^\perp\rangle, \, |a^\perp, B\rangle, \, |a^\perp, B^\perp\rangle\Big\} . \tag{3.24}$$

The basis $\mathcal{B}_0$ is a direct product basis while the basis $\mathcal{B}_1$ is not.

Case 2: If $|\psi_3\rangle = |b\rangle$ in (3.21) is chosen skew to $|a\rangle$, it follows that the state $|\psi_4\rangle$ must be orthogonal to $|b\rangle$. Assuming that the state $|\psi_4\rangle$ is not orthogonal to any of the three states $|b\rangle, |a\rangle$ and $|a^\perp\rangle$, the state $|\phi_4\rangle$ must be orthogonal to $|\phi_1\rangle, |\phi_2\rangle$ and $|\phi_3\rangle$. This is only possible if $|\phi_1\rangle = |\phi_2\rangle = |\phi_3\rangle$, implying that the states $|a, \phi_1\rangle$ and $|b, \phi_3\rangle$ are *not* orthogonal. Therefore, we must indeed have that $|\psi_4\rangle = |b^\perp\rangle$, leading to

$$\Big\{|a, \phi_1\rangle, \, |a^\perp, \phi_2\rangle, \, |b, \phi_3\rangle, \, |b^\perp, \phi_4\rangle\Big\} . \tag{3.25}$$

The orthogonality conditions

$$\langle\phi_1|\phi_3\rangle = \langle\phi_1|\phi_4\rangle = 0 \tag{3.26}$$

imply that both $|\phi_3\rangle$ and $|\phi_4\rangle$ must be orthogonal to $|\phi_1\rangle$, which allows us to conclude from

$$\langle\phi_2|\phi_3\rangle = \langle\phi_2|\phi_4\rangle = 0 \tag{3.27}$$

that $|\phi_2\rangle \equiv |\phi_1\rangle$. Now letting $|\phi_1\rangle = |A\rangle$, we find another family of indirect product bases,

$$\mathcal{B}_2 = \Big\{|a, A\rangle, \, |a^\perp, A\rangle, \, |b, A^\perp\rangle, \, |b^\perp, A^\perp\rangle\Big\} , \tag{3.28}$$

where $|a\rangle$ and $|b\rangle$ are skew. This concludes the construction of all product bases in dimension four. The basis $\mathcal{B}_0$ is a direct product basis while the bases $\mathcal{B}_1$ and $\mathcal{B}_2$ are not. After performing suitable LETs, we can thus summarise the complete list of product bases in dimension four as follows.

Lemma 3.2.1. *Any orthonormal product basis of the space $\mathbb{C}^2 \otimes \mathbb{C}^2$ is equivalent to a member of one of the families*

$$\begin{aligned} \mathcal{I}_0 &= \{|j_z, k_z\rangle\} \,, \\ \mathcal{I}_1 &= \{|0_z, k_z\rangle, |1_z, \hat{u}k_z\rangle\} \,, \\ \mathcal{I}_2 &= \{|j_z, 0_z\rangle, |\hat{v}j_z, 1_z\rangle\} \,, \end{aligned} \tag{3.29}$$

where the operators $\hat{u}, \hat{v} \in SU(2)$ act on the space $\mathbb{C}^2$ such that the states $|0_z\rangle$ and $\hat{u}|0_z\rangle$, as well as the states $|0_z\rangle$ and $\hat{v}|0_z\rangle$, are skew.

Note that the parameters on which the operators depend have been chosen in such a way that no product basis occurs more than once. A number of LETs (cf. Sec. 3.1.1) have been used to bring the bases into the form given in the lemma. The basis $\mathcal{B}_0$ in (3.23) has been mapped to $\mathcal{I}_0$ by means of a transformation $\hat{u}_1 \otimes \hat{u}_2$ such that $\hat{u}_1$ maps the pair of states $\{|a\rangle, |a^\perp\rangle\}$ to the standard basis $\{|j_z\rangle\}$ of $\mathbb{C}^2$, and $\hat{u}_2$ is defined analogously. Thus, the bases $\mathcal{B}_0$ and $\mathcal{I}_0$ are equivalent to each other. We apply a similar transformation to the basis $\mathcal{B}_1$ in (3.24) mapping two of the bases to the standard basis. The freedom to choose a third basis, associated with the pair $\{|B\rangle, |B^\perp\rangle\}$, is represented in $\mathcal{I}_1$ by the undetermined unitary operator $\hat{u}$ acting on the standard basis. The same reasoning brings $\mathcal{B}_2$ into the form (3.29) except that the roles of the two spaces are swapped. Since a complex conjugation reflects points on the Bloch sphere about the xz-plane, only half of all the unitaries $\hat{u}$ (and $\hat{v}$) need to be considered in Lemma 3.2.1. In other words, the bases associated with the unitaries $\hat{u}$ and $\hat{u}^*$, given by the complex conjugate of the matrix representing $\hat{u}$ in the z-basis, coincide.

The symmetry of the space $\mathbb{C}^2 \otimes \mathbb{C}^2$ is reflected in the fact that we found two bases $\mathcal{I}_1$ and $\mathcal{I}_2$ which are identical except for the order of the factors. If we stick with the idea that LETs dictate whether two product bases are equivalent to each other, we need to consider these bases as inequivalent. Thus, the complete set of product bases consists of two families each of which depends on two parameters due to the $SU(2)$-transformations $\hat{u}$ and $\hat{v}$. Not all three parameters of a transformation in $SU(2)$ are relevant since the overall phase of quantum states is physically irrelevant: each pair of opposite points on the Bloch sphere defines an orthonormal basis of $\mathbb{C}^2$ so that the set of all bases depends on only two real parameters. Note that the sets $\mathcal{I}_1$ and $\mathcal{I}_2$ of Lemma 3.2.1 are both connected to the product basis $\mathcal{I}_0$.

The symmetry becomes particularly obvious if we represent the bases of Lemma 3.2.1 by quantum circuits. The idea is to visualise the operation needed to map the states of the standard product basis $\mathcal{I}_0$ into the desired product basis by means of a quantum gate. This is always possible since any two orthonormal bases are connected by a unitary operation. Obviously, the trivial gate, described by the identity $\hat{I}$, maps the four vectors of the standard product basis to itself. Fig. (3.1) shows that (non-local) controlled-$\hat{u}$ and controlled-$\hat{v}$ gates are required to output the bases $\mathcal{I}_1$ and $\mathcal{I}_2$, respectively. As expected, the two circuits are identical upon swapping the qubits.

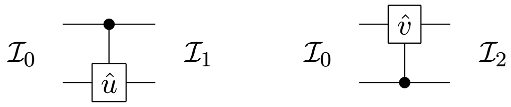

Figure 3.1: Two quantum circuits to create the product bases $\mathcal{I}_1$ and $\mathcal{I}_2$, respectively; the unitaries $\hat{u}$ and $\hat{v}$ only act on the target qubit if the control qubit is in the state $|1_z\rangle$.

3.2.2 All product bases in $d = 6$

To construct all product bases in dimension six we use the same method as in dimension four. Any product basis in the space $\mathbb{C}^2 \otimes \mathbb{C}^3$ takes the form

$$\Big\{|\psi_1, \Psi_1\rangle,\, |\psi_2, \Psi_2\rangle,\, |\psi_3, \Psi_3\rangle,\, |\psi_4, \Psi_4\rangle,\, |\psi_5, \Psi_5\rangle,\, |\psi_6, \Psi_6\rangle\Big\}\,, \tag{3.30}$$

with states $|\psi_n\rangle \in \mathbb{C}^2$ and $|\Psi_n\rangle \in \mathbb{C}^3$ for $n = 1\ldots6$, satisfying the orthogonality conditions

$$\langle\psi_n, \Psi_n|\psi_{n'}, \Psi_{n'}\rangle = \langle\psi_n|\psi_{n'}\rangle\langle\Psi_n|\Psi_{n'}\rangle = \delta_{nn'}\,, \quad n, n' = 1\ldots6\,. \tag{3.31}$$

The states $|\psi_n\rangle\,, n = 1\ldots6$, in (3.30) must contain at least *two* (not necessarily different) pairs of orthogonal states. If they do not, the orthogonality conditions require *four* orthogonal states in $\mathbb{C}^3$, which do not exist. In fact, the remaining two states in $\mathbb{C}^2$

must also be orthogonal, which implies that the product bases of $\mathbb{C}^6$ will come in three flavours. The states $|\psi_n\rangle, n = 1 \ldots 6$, fall into three pairs of states consisting of either three, two, or only one pair of orthonormal bases. The following lemma summarises the results of the detailed arguments given in Appendix A.

Lemma 3.2.2. *Any orthonormal product basis of the space $\mathbb{C}^2 \otimes \mathbb{C}^3$ is equivalent to a member of one of the families*

$$\begin{aligned}
\mathcal{I}_0 &= \{|j_z, J_z\rangle\} , \\
\mathcal{I}_1 &= \{|0_z, J_z\rangle, |1_z, \hat{U} J_z\rangle\} , \\
\mathcal{I}_2 &= \{|j_z, 0_z\rangle, |\hat{u}0_z, 1_z\rangle, |\hat{u}0_z, 2_z\rangle, |\hat{u}1_z, \hat{V}1_z\rangle, |\hat{u}1_z, \hat{V}2_z\rangle\} , \\
\mathcal{I}_3 &= \{|j_z, 0_z\rangle, |\hat{v}j_z, 1_z\rangle, |\hat{w}j_z, 2_z\rangle\} ,
\end{aligned} \tag{3.32}$$

with $j = 0, 1$ and $J = 0, 1, 2$; the operators $\hat{u}, \hat{v}, \hat{w} \in SU(2)$ and $\hat{U}, \hat{V} \in SU(3)$ act on $\mathbb{C}^2$ and $\mathbb{C}^3$, respectively, with $\hat{V}$ leaving the the state $|0_z\rangle$ invariant; the parameters of the operators $\hat{u}, \ldots, \hat{V}$ are chosen in such a way that no product basis occurs more than once.

Without any restrictions on the five unitary operators $\hat{u}, \ldots, \hat{V}$ some product bases would occur more than once in this list. For example, if $\hat{U} \equiv \hat{I}$, the basis $\mathcal{I}_1$ turns into $\mathcal{I}_0$; similarly, the bases associated with $\hat{U}$ and $\hat{U}^*$ are identical. We could remove such multiple occurrences by appropriately restricting the unitary operators but it is rather cumbersome to do so and not particularly informative.

Compared to dimension four, the number of families of indirect product bases have increased, and they contain transformations generated by elements of the group $SU(3)$. Clearly, there is no scope for symmetry under exchanging the two spaces of the product $\mathbb{C}^2 \otimes \mathbb{C}^3$. The families $\mathcal{I}_1$ to $\mathcal{I}_3$ each depend on a number of free parameters: $\mathcal{I}_1$ has six free parameters due to the unitary $\hat{U}$; two free parameters are associated with each $SU(2)$-transformation present in $\mathcal{I}_3$, while $\mathcal{I}_2$ is a five-parameter family – the transformations due to $\hat{V}$, which is effectively an $SU(2)$-transformation, brings not only two but *three* parameters because the overall phase of the states in the two-dimensional subspace spanned by $|1_z\rangle$ and $|2_z\rangle$ does *not* drop out. Figs. (3.2) and (3.3) show quantum circuits to generate the inequivalent product bases in dimension six.

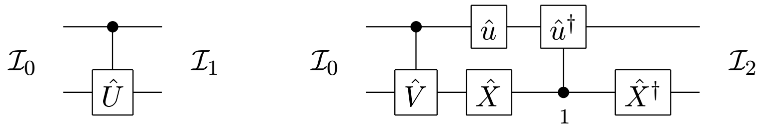

Figure 3.2: Quantum circuits for a qubit (upper wire) and qutrit (lower wire) to create the bases $\mathcal{I}_1$ and $\mathcal{I}_2$, respectively; the controlled-$\hat{U}$ and controlled-$\hat{V}$ gate act on the qutrit only if the control qubit is in the state $|1_z\rangle$; the unitary $\hat{u}^\dagger$, the adjoint of $\hat{u}$, acts on the qubit only when the control qutrit is in the state $|1_z\rangle$; and the operator $\hat{X}$ acts as a shift on the standard basis of $\mathbb{C}^3$.

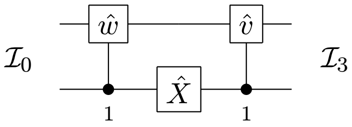

Figure 3.3: A quantum circuit for a qubit (upper wire) and qutrit (lower wire) to create the basis $\mathcal{I}_3$; the unitaries $\hat{v}$ and $\hat{w}$ act on the qubit only if the control qutrit is in the state $|1_z\rangle$, and the operator $\hat{X}$ acts as a shift on the standard basis of $\mathbb{C}^3$.

3.3 Adding MU product states to sets of orthogonal product vectors

In this section we derive a theorem which will play a crucial role in the construction of *all* pairs and triples of MU product bases in dimension four and six. This theorem is inspired by a constraint on two *direct* product bases to be MU, obtained in [93]:

Lemma. *Two [direct] product bases $\{|j_a, J_a\rangle\}$ and $\{|k_b, K_b\rangle\}$ in dimension $d = pq$ are MU if and only if $|j_a\rangle$ is MU to $|k_b\rangle$ in dimension p and $|J_a\rangle$ is MU to $|K_b\rangle$ in dimension q.*

This result does not cover *indirect* bases. To (partly) remedy this shortcoming, we will present two different ways to generalise this lemma. Firstly, we find a constraint on each product vector if it is to be MU to a specific set of product vectors; this result is obtained for spaces of arbitrary composite dimension $d = pq$. Secondly, we derive constraints on a product vector required to be MU to *any* (direct or indirect) given product basis of the spaces $\mathbb{C}^4$ or $\mathbb{C}^6$.

Consider p product states $\{|\psi_i, \Psi\rangle, i = 1 \dots p\}$ with an orthonormal basis $\{|\psi_i\rangle, i = 1 \dots p\}$ of the space $\mathbb{C}^p$, and with $|\Psi\rangle \in \mathbb{C}^q$. After swapping the two factors in Eq. (3.6), the product basis $\{|j_z, 0_z\rangle, |j_x, 1_z\rangle\}$, for example, is seen to consist of two sets of this form. We find that only particular product states can be MU to such sets of product states.

Lemma 3.3.1. *The product state $|\phi, \Phi\rangle$ in dimension $d = pq$ is MU to the set of orthogonal product states $\{|\psi_i, \Psi\rangle, i = 1 \dots p\}$ if and only if $|\phi\rangle$ is MU to $|\psi_i\rangle \in \mathbb{C}^p$ and $|\Phi\rangle$ is MU to $|\Psi\rangle \in \mathbb{C}^q$.*

If $|\langle\psi_i|\phi\rangle|^2 = 1/p$ and $|\langle\Psi|\Phi\rangle|^2 = 1/q$, then the product states are indeed MU in the space $\mathbb{C}^{pq}$ since it follows that $|\langle\psi_i, \Psi|\phi, \Phi\rangle|^2 = |\langle\psi_i|\phi\rangle|^2 |\langle\Psi|\Phi\rangle|^2 = 1/pq$. To prove the converse, we assume the product states are MU, $|\langle\psi_i, \Psi|\phi, \Phi\rangle|^2 = 1/pq$. Summing over $i = 1 \dots p$, we obtain $|\langle\Psi|\Phi\rangle|^2 = 1/q$ upon using the completeness relation $\sum_i |\langle\psi_i|\phi\rangle|^2 = 1$. This result immediately implies that $|\langle\psi_i|\phi\rangle|^2 = 1/p \, , i = 1 \dots p$, also holds.

Note that one can swap the roles of the factors in the tensor product. Then Lemma 3.3.1 restricts the form of any product state which is MU to a set of q orthogonal states $\{|\psi, \Psi_i\rangle, i = 1 \dots q\}$ with an orthonormal basis $\{|\Psi_i\rangle, i = 1 \dots q\}$ of the space $\mathbb{C}^q$, and with $|\psi\rangle \in \mathbb{C}^p$.

This result covers the lemma given at the beginning of this subsection. To see this, group the basis $\{|j_a, J_a\rangle\}$ into q sets of p orthonormal vectors $\{|j_a, 1_a\rangle\}$, $\{|j_a, 2_a\rangle\} \dots \{|j_a, q_a\rangle\}$; then, by Lemma 3.3.1, any product state $|\phi, \Phi\rangle$ is mutually unbiased to each set of vectors if and only if the state $|\phi\rangle$ is MU to all states $|j_a\rangle$, and the state $|\Phi\rangle$ is MU to all states $|J_a\rangle$. By replacing the state $|\phi, \Phi\rangle$ with a vector from the basis $\{|k_a, K_a\rangle\}$ and repeating the argument for all states in this basis, one arrives at the lemma for *direct* product bases.

The following generalisation uses the fact that we know all direct and indirect product bases in dimensions four and six.

Theorem 3.3.2. *The product state* $|\phi, \Phi\rangle \in \mathbb{C}^d, d \equiv pq \leq 6,$ *is MU to the product basis* $\{|\psi_i, \Psi_i\rangle\}$ *with* $i = 1 \ldots pq$, *if and only if* $|\phi\rangle$ *is MU to* $|\psi_i\rangle \in \mathbb{C}^p$ *and* $|\Phi\rangle$ *is MU to* $|\Psi_i\rangle \in \mathbb{C}^q$.

We prove this statement by considering the cases $d = 4$ and $d = 6$ separately:

• $d = 4$: All product bases in dimension four are given by the bases $\mathcal{I}_0, \mathcal{I}_1$ and $\mathcal{I}_2$, collected in Lemma 3.2.1. Each of these bases can be divided into groups of states of the form $\{|\psi_j, \Psi\rangle, j = 1, 2\}$, or $\{|\psi, \Psi_j\rangle, j = 1, 2\}$. Thus, Theorem 3.3.2 follows immediately from Lemma 3.3.1.

• $d = 6$: It is sufficient to consider the four families of bases given in Lemma 3.2.2. Each of the bases $\mathcal{I}_0$, $\mathcal{I}_1$ and $\mathcal{I}_3$ can be split into sets of the form required to apply Lemma 3.3.1; thus, Theorem 3.3.2 holds for these bases. To complete the proof, we need to consider the basis $\mathcal{I}_2$ which has no such decomposition. To begin, suppose that the basis $\mathcal{I}_2$ *is* MU to the state $|\phi, \Phi\rangle$. According to Lemma 3.3.1 this state is MU to the pair $\{|j_z, 0_z\rangle\}$ if both $|\langle\phi|0_z\rangle|^2 = |\langle\phi|1_z\rangle|^2 = 1/2$ and $|\langle\Phi|0_z\rangle|^2 = 1/3$ hold. The state $|\phi, \Phi\rangle$ also needs to satisfy

$$|\langle\phi|\hat{u}0_z\rangle|^2 |\langle\Phi|1_z\rangle|^2 = |\langle\phi|\hat{u}0_z\rangle|^2 |\langle\Phi|2_z\rangle|^2 = \frac{1}{6}\,; \tag{3.33}$$

adding these two constraints we find

$$|\langle\phi|\hat{u}0_z\rangle|^2 \Big(|\langle\Phi|1_z\rangle|^2 + |\langle\Phi|2_z\rangle|^2\Big) = \frac{1}{3}\,. \tag{3.34}$$

Using $\sum_J |\langle\Phi|J_z\rangle|^2 = 1$, i.e. the completeness relation of the basis $\{|J_z\rangle\}$, and $|\langle\Phi|0_z\rangle|^2 = 1/3$, we find that $|\langle\Phi|1_z\rangle|^2 + |\langle\Phi|2_z\rangle|^2 = 2/3$. Substituting this identity into (3.34) leaves us with $|\langle\phi|\hat{u}0_z\rangle|^2 = 1/2$, so that $|\langle\Phi|1_z\rangle|^2 = |\langle\Phi|2_z\rangle|^2 = 1/3$ as well. A similar argument applied to the pair $\{|\hat{u}1_z, \widehat{V1}_z\rangle, |\hat{u}1_z, \hat{V}2_z\rangle\}$ shows that indeed $|\langle\phi|\hat{u}1_z\rangle|^2 = 1/2$ and $|\langle\Phi|\hat{V}1_z\rangle|^2 = |\langle\Phi|\hat{V}2_z\rangle|^2 = 1/3$, which confirms that the state $|\phi, \Phi\rangle$ is of the desired form. The *converse* direction of the statement is straightforward.

We conjecture Theorem 3.3.2 to hold for *all* product dimensions $d \equiv pq$, i.e. $d = 4, 6, 9, 10, \ldots$ However, a proof similar to the one for $d = 4, 6$, would rely on the structure of all product bases in composite dimensions $d > 6$ – which is not known to us.

3.4 MU product bases in dimension four

3.4.1 All pairs of MU product bases

To construct *pairs* of MU product bases in the space $\mathbb{C}^4$, we check all possibilities to form MU pairs of the product bases displayed in Lemma 3.2.1 of Sec. 3.2.1. We find two families of locally inequivalent MU product bases given in Proposition 3.4.1 below. Since the bases $\mathcal{I}_1$ and $\mathcal{I}_2$ are identical to each other after a swap of factors, we only need to work through four different cases.

• $\{\mathcal{I}_0; \mathcal{B}_0\}$: Choose the second basis to be $\mathcal{B}_0$ given in Eq. (3.23). The eight vectors of the pair $\{\mathcal{I}_0; \mathcal{B}_0\}$ need to satisfy a total of 16 conditions, spelled out in Eq. (3.5) for $p = q = 2$ and with $|a\rangle$ skew to $|b\rangle$; however, not all of these conditions are independent. Summing $|\langle a, A|j_z, k_z\rangle|^2 = |\langle a|j_z\rangle|^2 \, |\langle A|k_z\rangle|^2 = 1/4$ over $j = 0, 1$, and $k = 0, 1$, respectively, leads to the four conditions

$$|\langle a|j_z\rangle|^2 = \frac{1}{2}\,, \quad j = 0, 1, \quad \text{and} \quad |\langle A|k_z\rangle|^2 = \frac{1}{2}\,, \quad k = 0, 1\,. \tag{3.35}$$

Thus, the states $|a\rangle$ and $|A\rangle$ must be linear combinations of the states $|0_z\rangle$ and $|1_z\rangle$ with coefficients of modulus $1/\sqrt{2}$,

$$|a\rangle = \frac{1}{\sqrt{2}}(|0_z\rangle + e^{i\mu}|1_z\rangle) \equiv \hat{r}_\mu|j_x\rangle\,, \quad \text{and} \quad |A\rangle = \hat{r}_\nu|j_x\rangle\ , \quad \mu, \nu \in [0, \pi)\,. \tag{3.36}$$

States of this form are located on the equator of the Bloch sphere. However, for given values of μ and ν these states can be transformed simultaneously by appropriate rotations about the z-axes, i.e. by a local unitary transformation $\hat{r}_\mu^\dagger \otimes \hat{r}_\nu^\dagger$, into the state $|0_x, 0_x\rangle$, thus mapping $\mathcal{B}_0$ into the basis $\{|j_x, k_x\rangle\}$. Not surprisingly, all pairs of MU bases constructed from two copies of the *direct* product basis are found to be equivalent to the Heisenberg-Weyl pair

$$\mathcal{P}_0^{(4)} = \{|j_z, k_z\rangle;\ |j_x, k_x\rangle\}\,. \tag{3.37}$$

• $\{\mathcal{I}_0;\mathcal{B}_1\}$ and $\{\mathcal{I}_0;\mathcal{B}_2\}$: These two cases will be covered by $\{\mathcal{I}_2;\mathcal{B}_1\}$ and $\{\mathcal{I}_1;\mathcal{B}_2\}$, respectively, since we will treat the direct product basis $\mathcal{I}_0$ as a subset of both $\mathcal{I}_1$ and $\mathcal{I}_2$.

• $\{\mathcal{I}_1;\mathcal{B}_1\}$ and $\{\mathcal{I}_2;\mathcal{B}_2\}$: The bases $\mathcal{I}_1$ and $\mathcal{B}_1$ are MU only if the two distinct bases $\{|A\rangle,|A^\perp\rangle\}$ and $\{|B\rangle,|B^\perp\rangle\}$ are both MU to the standard basis $\{|k_z\rangle\}$ as well as to $\{|\hat{u}k_z\rangle\}$. The basis $\mathcal{B}_1$ can be mapped, by local transformations, into the basis $\{|0_x,k_x\rangle,|1_x,\hat{r}_\nu k_x\rangle\}$, but with the condition that the pair of states $\{|\hat{r}_\nu k_x\rangle\}$ is MU to the pair $\{|\hat{u}k_z\rangle\}$. This condition is only satisfied if $\{|\hat{r}_\nu k_x\rangle\}$ is one of the bases $\{|j_x\rangle\}$ or $\{|j_y\rangle\}$. Either choice for the basis $\{|\hat{r}_\nu k_x\rangle\}$ implies that one of the bases $\mathcal{I}_1$ or $\mathcal{B}_1$ is a direct product basis. Thus, we cannot construct a pair of MU bases out of the bases $\mathcal{I}_1$ and $\mathcal{B}_1$. Since $\{\mathcal{I}_2;\mathcal{B}_2\}$ is obtained from $\{\mathcal{I}_1;\mathcal{B}_1\}$ by a swap of the qubits involved, these bases also do not combine to a pair of MU product bases.

• $\{\mathcal{I}_1;\mathcal{B}_2\}$ and $\{\mathcal{I}_2;\mathcal{B}_1\}$: We now combine the basis $\mathcal{I}_1=\{|0_z,k_z\rangle,\,|1_z,\hat{u}k_z\rangle\}$ with the basis

$$\mathcal{B}_2=\Big\{|a,A\rangle,\,|a^\perp,A\rangle,\,|b,A^\perp\rangle,\,|b^\perp,A^\perp\rangle\Big\}\,. \tag{3.38}$$

Lemma 3.3.1 implies that the states of $\mathcal{B}_2$ are MU to the states $\{|0_z,k_z\rangle\}$ contained in $\mathcal{I}_1$ if we have

$$|a\rangle=\hat{r}_\lambda|j_x\rangle\,,\quad|b\rangle=\hat{r}_\nu|j_x\rangle\,,\quad|A\rangle=\hat{r}_\xi|j_x\rangle\,, \tag{3.39}$$

with $\lambda,\nu,\xi\in[0,\pi)$. Now map the state $|a,A\rangle$ to $|0_x,0_x\rangle$ by the local unitary transformation $\hat{r}_\lambda^\dagger\otimes\hat{r}_\xi^\dagger$ to write $\mathcal{B}_2$ as

$$\mathcal{B}_2=\Big\{|j_x,0_x\rangle,\,|\hat{r}_\nu j_x,1_x\rangle\Big\}\,, \tag{3.40}$$

where the unitary operator $\hat{r}_\nu$ rotates the x-basis $\{|j_x\rangle\}\equiv\{|\pm\rangle\}$ into the xy-plane according to $\hat{r}_\nu|\pm\rangle=(|0_z\rangle\pm e^{i\nu}|1_z\rangle)/\sqrt{2}$, where $\nu\in(0,\pi)$. Finally, the remaining pair of states in $\mathcal{I}_1$, viz. $\{|1_z,\hat{u}k_z\rangle\}$, is MU to the pair $\{|\hat{r}_\nu j_x,1_x\rangle\Big\}$ only if $\{|\hat{u}k_z\rangle\}\equiv\{|\hat{s}_\mu k_z\rangle\}$ where $\hat{s}_\mu$ is a rotation about the x-axis of the Bloch sphere. Thus, we have obtained a two-parameter family of product bases

$$\mathcal{P}_1^{(4)}=\{|0_z,k_z\rangle,|1_z,\hat{s}_\mu k_z\rangle;\,|j_x,0_x\rangle,|\hat{r}_\nu j_x,1_x\rangle\}\,, \tag{3.41}$$

with rotations $\hat{r}_\nu$, $\nu \in (0,\pi)$, and $\hat{s}_\mu$, $\mu \in [0,\pi)$, about the z- and x-axes, respectively.

The pair $\mathcal{P}_1^{(4)}$ has a partner that is obtained from constructing MU product pairs using $\{\mathcal{I}_2; \mathcal{B}_1\}$. However, due to the symmetry, it is found readily from swapping the two spaces $\mathbb{C}^2$ in Eq. (3.41),

$$\{|0_z, k_z\rangle, |\hat{s}_{\mu'} j_z, 1_z\rangle;\ |0_x, k_x\rangle, |1_x, \hat{r}_{\nu'} k_x\rangle\}\,, \tag{3.42}$$

with unitaries $\hat{r}_{\nu'}$ and $\hat{s}_{\mu'}$ defined in analogy to the operators used in the definition of $\mathcal{P}_1^{(4)}$. This pair turns out to be equivalent to $\mathcal{P}_1^{(4)}$ by multiplying (3.42), from the left, with a unitary $\hat{t}_\rho \otimes \hat{t}_\rho$, where $\hat{t}_\rho$ is a rotation about the y-axis. Choosing $\rho = \pi/2$ such that $\{|\hat{t}_{\pi/2} j_x\rangle\} = \{|j_z\rangle\}$, the MU product pair transforms into $\mathcal{P}_1^{(4)}$. We now collect our findings regarding MU product bases in dimension four.

Proposition 3.4.1. *Any pair of MU product bases in the space $\mathbb{C}^2 \otimes \mathbb{C}^2$ is equivalent to a member of the families*

$$\begin{aligned}
\mathcal{P}_0^{(4)} &\equiv \{|j_z, k_z\rangle;\ |j_x, k_x\rangle\}\,,\\
\mathcal{P}_1^{(4)} &\equiv \{|0_z, k_z\rangle, |1_z, \hat{s}_\mu k_z\rangle;\ |j_x, 0_x\rangle, |\hat{r}_\nu j_x, 1_x\rangle\}\,,
\end{aligned} \tag{3.43}$$

where $j, k = 0, 1$, and the unitary operator $\hat{r}_\nu$ rotates the basis $\{|j_x\rangle\} \equiv \{|k_x\rangle\} \equiv \{|\pm\rangle\}$ into the xy-plane according to $\hat{r}_\nu|\pm\rangle = (|0_z\rangle \pm e^{i\nu}|1_z\rangle)/\sqrt{2}$ for $\nu \in (0,\pi)$; the operator $\hat{s}_\mu$ generates rotations about the x-axis, i.e. $\hat{s}_\mu|k_z\rangle = (|0_x\rangle + (-1)^k e^{i\mu}|1_x\rangle)/\sqrt{2}$ for $\mu \in [0,\pi)$.

The pair $\mathcal{P}_0^{(4)}$ is the Heisenberg-Weyl pair consisting of two direct product bases. The pair of MU bases $\mathcal{P}_1^{(4)}$ is a *two-parameter* family and may contain direct and indirect product bases. Notice that the operator $\hat{s}_\mu$ can act as the identity since the first basis of $\mathcal{P}_1^{(4)}$ may be the standard basis $\{|j_z, k_z\rangle\}$.

The pair $\mathcal{P}_1^{(4)}$ turns out to be *equivalent* under *non-local* transformations to the Fourier family as follows from mapping the first basis to the standard basis $\{|j_z, k_z\rangle\}$. Thus, we have obtained all pairs of MU bases in dimension four (cf. Sec. 3 of [19]) in spite of limiting ourselves initially to MU product bases only.

3.4.2 All triples of MU product bases

Now we are in a position to derive all triples of MU product bases in dimension $d = 4$: we need to determine which of the pairs of MU product bases given in Proposition 3.4.1 can be extended by a third MU product basis.

It is easy to see that the MU pair $\mathcal{P}_0^{(4)} \equiv \{|j_z, k_z\rangle;\ |j_x, k_x\rangle\}$ can be extended by adjoining a third direct product basis, namely $|j_y, k_y\rangle$, resulting in the standard Heisenberg-Weyl triple. This is the *only* possibility, as follows immediately from Theorem 3.3.2: a product state $|\phi, \Phi\rangle$ is MU to both $\{|j_z, k_z\rangle\}$ and $\{|j_x, k_x\rangle\}$ only if $|\phi\rangle$ is MU both to $\{|j_z\rangle\}$ and $\{|j_x\rangle\}$, and if $|\Phi\rangle$ is MU both to $\{|k_z\rangle\}$ and $\{|k_x\rangle\}$.

The pair $\mathcal{P}_1^{(4)}$ of MU bases cannot be extended, not even by a single MU product state. To extend the pair by an MU product state, one would need to find a state in $\mathbb{C}^2$ which is MU to the three bases $\{|k_z\rangle\}$, $\{|k_x\rangle\}$ and $\{|\hat{r}_\nu k_x\rangle\}$. Since $\nu \in (0, \pi)$, no two of these three bases coincide and there is no state in the space $\mathbb{C}^2$ simultaneously MU to three distinct bases. As a consequence, the number of MU product triples is rather limited in dimension four.

Proposition 3.4.2. *Any triple of MU product bases in the space $\mathbb{C}^2 \otimes \mathbb{C}^2$ is equivalent to*

$$\mathcal{T}_0^{(4)} \equiv \{|j_z, k_z\rangle;\ |j_x, k_x\rangle;\ |j_y, k_y\rangle\}\ . \tag{3.44}$$

Using Theorem 3.3.2 again, the non-existence of even a single product state MU to the triple $\mathcal{T}_0^{(4)}$ follows immediately – all states MU to the triple must be entangled.

This observation agrees with results reported earlier. For the two-qubit system considered here, a construction of the five MU bases based on the Galois field $GF(4)$ has been given in [54]. The complete sets obtained turn out to be equivalent under local unitary transformations, and they necessarily consist of three MU bases made up from separable (i.e. product) bases while the remaining two contain maximally entangled states only. This structure also emerges from an approach which exploits the fact that any *complete* set of MU bases of a bipartite system in $\mathbb{C}^d$ contains a *fixed* d-dependent amount of entanglement (see Sec. 2.4.2). When $d = 4$, this result implies that for a complete set of MU bases containing the triple $\mathcal{T}_0^{(4)}$, the other two bases of the quintuple must consist of *entangled* states – in fact, only maximally entangled states are permitted. In [58], the entanglement structure of complete sets of MU bases related to Heisenberg-Weyl operators in prime-power dimensions has been studied, leading to a generalisation of the result for dimension $d = 4$: in bipartite systems of dimension $d = p^2$, if $(p+1)$ MU bases consist of product states, the remaining bases contain only maximally entangled states.

3.5 MU product bases in dimension six

3.5.1 All pairs of MU product bases

We will now construct all pairs of MU product bases in dimension six following the method used in dimension four (cf. Sec. 3.2.1). To obtain a MU pair we take each basis listed in Lemma 3.2.2 and go through all possibilities of adding one of the product bases $\mathcal{B}_0$ to $\mathcal{B}_3$ (cf. Eqs. (A.5,A.4,A.8,A.9) of Appendix A).

When constructing pairs of MU product bases, it is not necessary to include the basis $\mathcal{I}_2$ in Lemma 3.2.2. We will show now that the operator $\hat{V}$ must either act as the identity on the pair of states $\{|1_z\rangle, |2_z\rangle\}$ or swap them, i.e. only $\alpha = 0$ or $\beta = 0$ are allowed in the expression $\hat{V}|1_z\rangle = \alpha|1_z\rangle + \beta|2_z\rangle$. However, in both cases the simplified product basis $\mathcal{I}_2$ turns into a special case of $\mathcal{I}_3$, given in (3.32).

Here is the reason why the operator $\hat{V}$ must simplify in the way just described. Apply Theorem 3.3.2 to the product state $|\phi, \Phi\rangle$ required to be MU to $\mathcal{I}_2$: the state $|\Phi\rangle$ must be MU to all six vectors of $\mathbb{C}^3$ present in $\mathcal{I}_2$. Consequently, all states in $\mathbb{C}^3$ which occur in the bases $\mathcal{B}_0$ to $\mathcal{B}_3$, defined in Eqs. (A.5,A.4,A.8,A.9) – these are all candidates for a second product basis MU to $\mathcal{I}_2$ – must be MU to the standard basis $\{|J_z\rangle\}$ of $\mathbb{C}^3$. Now, each of these four bases contains another orthonormal basis of $\mathbb{C}^3$, namely $\{|A\rangle, |A^\perp\rangle, |A^{\perp\perp}\rangle\}$. There is a two-parameter family of such states, given in (3.15). However, these states must also be MU to the state $\hat{V}|1_z\rangle$ of the basis $\mathcal{I}_2$. For the states $|A\rangle$ and $|A^{\perp}\rangle$, this requirement reads

$$|\langle A|(\alpha|1_z\rangle+\beta|2_z\rangle)|^2 = |\langle A^{\perp}|(\alpha|1_z\rangle+\beta|2_z\rangle)|^2 = \frac{1}{3}\,. \tag{3.45}$$

Now using the explicit expressions of the states $|A\rangle$ and $|A^{\perp}\rangle$ given in (3.16) and the identity $|\alpha|^2+|\beta|^2=1$, the first equality leads to

$$|1+\omega|\,|\alpha|\,|\beta| = |\alpha|\,|\beta|\,, \tag{3.46}$$

which implies that either $\alpha\equiv 0$ or $\beta\equiv 0$. Thus, for the construction of pairs it is sufficient to use the restricted basis

$$\mathcal{I}_2' = \{|j_z,0_z\rangle, |\hat{u}j_z,1_z\rangle, |\hat{u}j_z,2_z\rangle\} \tag{3.47}$$

instead of $\mathcal{I}_2$ given in Lemma 3.2.2. All bases of this form, however, are contained in $\mathcal{I}_3$ if one chooses $\hat{v}=\hat{w}\equiv\hat{u}$ in (3.32). This simplification also holds for the basis $\mathcal{B}_2$ when occurring in a pair of product bases.

The actual derivation of all MU product bases in dimension six is lengthy but straightforward. The calculations have been relegated to Appendix B except for the pairing of the basis $\mathcal{I}_1$ with $\mathcal{B}_1$, which gives rise to the pair $\mathcal{P}_2$. The proof that no other (non-trivial) pair of MU product bases results from $\{\mathcal{I}_1;\mathcal{B}_1\}$ has been obtained by A. Sudbery, and it is given in Appendix C. We now summarise the results derived in these two appendices.

Theorem 3.5.1. *Any pair of MU product bases in the space $\mathbb{C}^2\otimes\mathbb{C}^3$ is equivalent to a member of the families*

$$\begin{aligned}
\mathcal{P}_0 &= \{|j_z,J_z\rangle;\ |j_x,J_x\rangle\}\,,\\
\mathcal{P}_1 &= \{|j_z,J_z\rangle;\ |0_x,J_x\rangle, |1_x,\hat{R}_{\xi,\eta}J_x\rangle\}\,,\\
\mathcal{P}_2 &= \{|0_z,J_z\rangle, |1_z,J_y\rangle;\ |0_x,J_x\rangle, |1_x,J_w\rangle\}\,,\\
\mathcal{P}_3 &= \{|0_z,J_z\rangle, |1_z,\hat{S}_{\zeta,\chi}J_z\rangle;\ |j_x,0_x\rangle, |\hat{r}_\sigma j_x,1_x\rangle, |\hat{r}_\tau j_x,2_x\rangle\}\,,
\end{aligned} \tag{3.48}$$

with $j=0,1$ and $J=0,1,2$. The unitary operator $\hat{R}_{\xi,\eta}$ is defined as $\hat{R}_{\xi,\eta}=|0_z\rangle\langle 0_z|+e^{i\xi}|1_z\rangle\langle 1_z|+e^{i\eta}|2_z\rangle\langle 2_z|$, for $\eta,\xi\in[0,2\pi)$, and $\hat{S}_{\zeta,\chi}$ is defined analogously with respect to the x-basis; the unitary operators $\hat{r}_\sigma$ and $\hat{r}_\tau$ act on the basis $\{|j_x\rangle\}\equiv\{|\pm\rangle\}$ according to $\hat{r}_\sigma|j_x\rangle=(|0_z\rangle\pm e^{i\sigma}|1_z\rangle)/\sqrt{2}$ for $\sigma\in(0,\pi)$, etc.

As before, the ranges of the parameters are assumed to be such that no MU product pair occurs more than once in the list. The pairs $\mathcal{P}_0$ and $\mathcal{P}_2$ have no parameter dependence, the pair $\mathcal{P}_1$ depends on two parameters, while $\mathcal{P}_3$ is a four-parameter family.

Theorem 3.5.1 represents the first main result of this chapter. It states that there are continuously many possibilities to select pairs of MU bases which, however, can be listed exhaustively. We will now proceed to *analytically* construct all *triples* of MU bases which exist in $d = 6$. This will lead to a non-existence result in Sec. 3.6, namely Theorem 3.6.1, which states the impossibility to extend any MU product triple by even a single MU vector. Thus, complete sets of MU bases in $d = 6$ will contain at most *pairs* of MU product bases.

An alternative method to exploit Theorem 3.5.1 will be persued in the next chapter. Upon using suitable *non-local* unitary transformations and known results obtained by computer-algebraic methods, the strongest possible statement about MU product bases is then derived: if a complete set of seven MU bases exists, it will contain at most *one* product basis – which may be chosen to be the standard basis.

3.5.2 All triples of MU product bases

It is straightforward to enlarge the existing pairs of MU product bases in Theorem 3.5.1 to triples: simply add the MU product bases listed in Lemma 3.2.2, one after the other, to each of the pairs $\mathcal{P}_0$ to $\mathcal{P}_3$ and check whether a valid MU product triple results.

Neither of the pairs $\mathcal{P}_2$ and $\mathcal{P}_3$ in Theorem 3.5.1 can be extended by a single MU product state. To do so, we would need a vector MU to the three distinct bases $\{|j_z\rangle\}$, $\{|j_x\rangle\}$ and $\{|\hat{r}_\sigma j_x\rangle\}$ in the space $\mathbb{C}^2$, or a vector mutually unbiased to four MU bases in the space $\mathbb{C}^3$. No such states exist, implying that any state mutually unbiased to these pairs must be entangled.

The pairs $\mathcal{P}_0$ and $\mathcal{P}_1$ *can* be extended by a further MU product basis since there exist vectors of the spaces $\mathbb{C}^2$ and $\mathbb{C}^3$ that satisfy the necessary conditions. To obtain the complete list of all MU product triples in $\mathbb{C}^6$ we thus need to search for possible extensions of these two pairs by a third product basis. Starting with $\mathcal{P}_0$, it is possible to extend this pair by either $\mathcal{B}_0$ or $\mathcal{B}_1$.

• $\{\mathcal{P}_0; \mathcal{B}_0\}$: If we choose the third basis to be of the form $\mathcal{B}_0$, there are only two choices, $\{|j_y, J_y\rangle\}$ or $\{|j_y, J_w\rangle\}$. Using the local complex conjugation $\hat{I} \otimes \hat{K}$, the resulting triples are found to be equivalent,

$$\{|j_z, J_z\rangle;\ |j_x, J_x\rangle;\ |j_y, J_y\rangle\} \sim \{|j_z, J_z\rangle;\ |j_x, J_x\rangle;\ |j_y, J_w\rangle\}\,; \tag{3.49}$$

consequently, all triples of this type are equivalent to the Heisenberg-Weyl triple

$$\mathcal{T}_0 = \{|j_z, J_z\rangle;\ |j_x, J_x\rangle;\ |j_y, J_y\rangle\}\,. \tag{3.50}$$

• $\{\mathcal{P}_0; \mathcal{B}_1\}$: If we extend $\mathcal{P}_0$ by an indirect product basis of the form $\mathcal{B}_1$, there are only two choices, $\{|0_y, J_y\rangle, |1_y, J_w\rangle\}$ or $\{|0_y, J_w\rangle, |1_y, J_y\rangle\}$. Again, a local complex conjugation $\hat{k} \otimes \hat{I}$ maps one of the triples into the other,

$$\{|j_z, J_z\rangle; |j_x, J_x\rangle;\ |0_y, J_y\rangle, |1_y, J_w\rangle\} \sim \{|j_z, J_z\rangle;\ |j_x, J_x\rangle;\ |0_y, J_w\rangle, |1_y, J_y\rangle\}\,, \tag{3.51}$$

leaving us with the triple

$$\mathcal{T}_1 = \{|j_z, J_z\rangle;\ |j_x, J_x\rangle;\ |0_y, J_y\rangle, |1_y, J_w\rangle\}\,. \tag{3.52}$$

Now turning to the pair $\mathcal{P}_1$, we again attempt to obtain a triple by adding either $\mathcal{B}_0$ or $\mathcal{B}_1$.

• $\{\mathcal{P}_1; \mathcal{B}_0\}$ or $\{\mathcal{P}_1; \mathcal{B}_1\}$: First, extend the pair $\mathcal{P}_1$ by a direct product basis, resulting in either $\{|j_z, J_z\rangle; |0_x, J_x\rangle, |1_x, J_y\rangle; |j_y, J_w\rangle\}$ or $\{|j_z, J_z\rangle; |0_x, J_x\rangle, |1_x, J_w\rangle; |j_y, J_y\rangle\}$. It is not difficult to apply suitable LETs to transform them into the triple $\mathcal{T}_1$. Now extend the pair $\mathcal{P}_1$ by an indirect product basis $\mathcal{B}_1$. This leads to a contradiction since we would need the states $\{|\hat{R}_{\xi,\eta} J_x\rangle\}$ in $\mathcal{P}_1$ to coincide with $\{|J_x\rangle\}$, which is not allowed.

This completes the construction of all MU product triples in dimension six, leading to the second main result of this chapter.

Theorem 3.5.2. *Any triple of MU product bases in the space $\mathbb{C}^2 \otimes \mathbb{C}^3$ is equivalent to either*

$$\begin{aligned} \mathcal{T}_0 &= \{|j_z, J_z\rangle;\ |j_x, J_x\rangle;\ |j_y, J_y\rangle\}\,, \\ \textit{or } \mathcal{T}_1 &= \{|j_z, J_z\rangle;\ |j_x, J_x\rangle;\ |0_y, J_y\rangle, |1_y, J_w\rangle\}\,. \end{aligned} \tag{3.53}$$

According to Theorem 3.3.2, neither of these triples can be extended by a single MU product state. Thus, any complete set of seven MU bases in dimension six will contain at most three product bases, and if it does, the triple must be equivalent to one of those in Theorem 3.5.2. In the following section we will obtain an even stronger result.

3.6 Excluding triples of MU product bases from complete sets

In this section we derive the third main result of this chapter.

Theorem 3.6.1. *No triple of MU product bases in dimension six can be extended by a single MU vector.*

In other words, no complete set of seven MU bases in $d = 6$ contains a triple of MU product bases. This result relies on a computer-aided proof in [34], which finds a total of 48 vectors MU to the pair of eigenbases of the Heisenberg-Weyl operators X_6 and Z_6, giving rise to sixteen different orthonormal bases (see Sec. 2.5.2). However, none of these bases allows one to extend the given pair beyond a triple of MU bases.

The present construction of MU product triples effectively produces twelve (and only twelve) product vectors that are MU to the pair $\mathcal{P}_0 = \{|j_z, J_z\rangle; |j_x, J_x\rangle\}$, namely $\{|j_y, J_y\rangle\}$ and $\{|j_y, J_w\rangle\}$, and they give rise to the only two inequivalent triples of MU bases, $\mathcal{T}_0$ and $\mathcal{T}_1$. Since $\mathcal{P}_0$ is equivalent to the eigenbases of X_6 and Z_6, clearly these twelve product vectors must figure among the 48 vectors given in [34].

To show this, we must first deal with a difference in our definition of the HW operators. The HW pair used in [34] does not have the same form as $\mathcal{P}_0$ since the x-basis in [34] is the eigenbasis of the operator X_6, whereas we have used the eigenbasis of the operator $X_2 \otimes X_3$ (cf. Eq. (2.12)). Nevertheless, both pairs of bases turn out to be equivalent using a *non-local* unitary transformation. By writing the operators as matrices, we find that $X_2 \otimes X_3 = P_{25} X_6 P_{25}$, where P_{25} is a permutation matrix permuting rows two and five. This non-local transformation brings the eigenbasis of X_6 into product form, i.e. $\{|j_x, J_x\rangle\}$, by multiplying it with P_{25} from the left.

The same transformation must also be applied to the list of 48 vectors so that they are MU to the pair $\mathcal{P}_0$. After multiplying each of these vectors by the matrix P_{25} from the left, one easily identifies the twelve product vectors, numbered by 1, 2, 5, 6, 9, 10, 13, 14, 17, 18, 21 and 22 in the Appendix of the updated version of [34]. For example, the vector labelled (1) transforms as follows:

$$\begin{aligned}\frac{1}{\sqrt{6}}P_{25}(1,\alpha^5,1,-\alpha^3,-\alpha^2,-\alpha^3)^{\mathrm{T}} =& \frac{1}{\sqrt{6}}(1,-\alpha^2,1,-\alpha^3,\alpha^5,-\alpha^3)^{\mathrm{T}} \\ \equiv& \frac{1}{\sqrt{6}}(1,\omega^2,1,-i,-i\omega^2,-i)^{\mathrm{T}} \\ \equiv& \frac{1}{\sqrt{6}}(1,-i)^{\mathrm{T}} \otimes (1,\omega^2,1)^{\mathrm{T}} \qquad (3.54)\end{aligned}$$

where $\alpha = e^{2\pi i/12}$ and $\omega = e^{2\pi i/3}$. This vector is the product state $|1_y, 1_y\rangle$.

The twelve vectors give rise to four of the sixteen orthonormal bases which are MU to the original pair. These product bases are covered by the product bases we construct when extending the Heisenberg-Weyl pair $\mathcal{P}_0$ to a triple; however, only two of the four triples are locally inequivalent as follows from exploiting suitable local equivalence transformations.

Upon combining the computer-aided result just described with Theorem 3.5.2 it is straightforward to arrive at a result that excludes product triples from being part of a complete set of seven MU bases. The triples of MU product bases $\mathcal{T}_0$ and $\mathcal{T}_1$ both contain the Heisenberg-Weyl pair $\mathcal{P}_0 = \{|j_z, J_z\rangle; |j_x, J_x\rangle\}$, and it is impossible to extend this pair by more than a single MU basis according to [34]. Since Theorem 3.5.2 provides an *exhaustive* list of MU triples in the space $\mathbb{C}^2 \otimes \mathbb{C}^3$, it follows that *no complete set of seven MU bases in* $d = 6$ *contains a triple of MU product bases.*

3.7 Summary

By limiting ourselves to orthonormal product bases, we have been able to obtain a number of analytic results regarding the existence of MU bases of the space $\mathbb{C}^2 \otimes \mathbb{C}^3$. After identifying all orthonormal product bases of this space, presented in Lemma 3.2.2, we have constructed an exhaustive list of pairs of MU product bases. They come in four different flavours according to Theorem 3.5.1. Next, Theorem 3.5.2 states that, in addition to the Heisenberg-Weyl triple, there is only one other locally inequivalent triple of MU product bases. The absence of quadruples of MU product bases agrees with Zauner's conjecture [98] that there are no more than three MU bases in dimension six.

The derivation of the list of MU product pairs and triples has been simplified considerably by the content of Theorem 3.3.2. It spells out severe restrictions on the form of product states required to be MU to certain sets of orthonormal states in the space $\mathbb{C}^2 \otimes \mathbb{C}^3$. We have established Theorem 3.3.2 for dimensions $d = 4$ and $d = 6$ only, since the proof relies on enumerating all orthonormal product bases in these dimensions.

Theorem 3.5.2 allows us to partly replicate results obtained by means of a computer-algebraic method. Out of the 48 vectors mutually unbiased to the Heisenberg-Weyl pair $\mathcal{P}_0$, found in [34], we successfully recover twelve, and they are shown to be equivalent to product vectors.

The most important consequence of exhaustively enumerating MU product bases in dimension six is a bound on their allowed number in complete sets of MU bases. Applying Theorem 3.3.2 to the triples of MU product bases in $\mathbb{C}^2 \otimes \mathbb{C}^3$, namely $\mathcal{T}_0$ and $\mathcal{T}_1$, directly implies that no single *product* state can be MU to any of them. However, a stronger result is within reach, spelled out in Theorem 3.6.1: it is impossible to complement either $\mathcal{T}_0$ or $\mathcal{T}_1$ by *any* MU vector. This follows from combining Theorem 3.5.2 with the results derived in [34]. Thus, *a complete set of MU bases in dimension six cannot contain a product triple.* This is in marked contrast to the prime-power dimension p^2 where a complete set of MU bases necessarily contains $(p + 1)$ MU product bases constructed from the tensor products of Heisenberg-Weyl operators [58].

A similar situation has been described in [5] where a different class of MU bases is studied. Given a "nice error basis", consisting of d^2 suitable matrices, one can construct MU bases from certain partitions of the matrices (see Sec. 2.4.1). In the case of dimension six, it is shown that any partition of a nice error basis gives rise to no more than three MU bases. This limitation and the non-existence of more that three

MU *product* bases are independent results: MU product bases and MU bases arising from nice unitary error bases are structurally different. For example, our construction reproduces the continuous family $\mathcal{P}_1^{(4)}$ of MU product pairs in $d = 4$, and it is known that some of the pairs in this family are *inequivalent* to MU bases stemming from nice error bases [53].

Our considerations are backed by deriving corresponding results in the Hilbert space of two qubits, i.e. $\mathbb{C}^2 \otimes \mathbb{C}^2$. In this case there exists a symmetry between the two factors and the enumeration of MU product pairs and triples is much simpler. Clearly, when a qubit is combined with a qutrit, no such symmetry exists. We believe that the symmetries between the subsystems present in only prime-power dimensions are the ultimate reason that additional "identities" exist which allow for the construction of *complete* sets of MU bases.

Let us conclude by formulating a conjecture which emerges naturally from our results: we expect Theorem 3.3.2 to hold for *all* composite dimensions $d = pq \geq 4$, not only for $d = 4$ and $d = 6$. Our pedestrian proof in these dimensions relies on enumerating all orthonormal product bases. However, the set of product bases in composite dimensions is likely to possess a certain structure which, once spelled out, should allow for a more elegant proof applicable to arbitrary composite dimensions.

Chapter 4

The limited role of MU product bases in dimension 6

The purpose of this chapter is to derive a rigorous result regarding the impossibility to extend certain pairs of MU bases in dimension six to complete sets. We will show that no *pair* of MU product bases can figure in a complete set, as stated by the following theorem.

Theorem 4.0.1. *If a complete set of seven MU bases in dimension six exists, it contains at most one product basis.*

This is, in fact, the *strongest possible* bound on the number of MU product bases since one can always map one MU basis of a complete set to the standard basis. The proof will start from the exhaustive list of pairs of MU product bases of $\mathbb{C}^6$ constructed in Section 3.5.1. Not all of the listed pairs are given in the standard form which requires the first basis to be the computational basis [18]. Thus, we will first bring the pairs of the list into standard form using unitary equivalence transformations. We will find that the second MU product basis of each pair is mapped either to a member of the Fourier family of Hadamard matrices or the isolated matrix S_6. Using several computer-aided results, it is then straightforward to prove Theorem 4.0.1.

To begin, we reproduce the set of pairs of MU product bases obtained in Section 3.5.1. It will be convenient to represent the MU product pairs of Theorem 3.5.1 in terms of (6×6) unitary matrices,

$$\mathcal{P}_0 = \{I;\, \widetilde{F}(0,0)\}\,, \tag{4.1}$$

$$\mathcal{P}_1 = \{I;\, \widetilde{F}^{\mathrm{T}}(\xi,\eta)\}\,, \tag{4.2}$$

$$\mathcal{P}_2 = \{\widetilde{I}(4\pi/3, 4\pi/3);\, \widetilde{F}^{\mathrm{T}}(4\pi/3, 4\pi/3)\}\,, \tag{4.3}$$

$$\mathcal{P}_3 = \{\widetilde{I}(\zeta,\chi);\, \widetilde{F}(\sigma,\tau)\}\,. \tag{4.4}$$

Here, the unitary matrix $\widetilde{F}(\xi,\eta)$ is given by

$$\widetilde{F}(\xi,\eta) = \frac{1}{\sqrt{2}} \begin{pmatrix} F_3 & F_3 \\ F_3 D & -F_3 D \end{pmatrix}, \tag{4.5}$$

with F_3 defined in Eq. (3.16) and the diagonal matrix $D = \mathrm{diag}(1, e^{i\xi}, e^{i\eta})$. This particular form of $\widetilde{F}(\xi,\eta)$ appears in [10]. The transpose of $\widetilde{F}$, present in $\mathcal{P}_1$ and $\mathcal{P}_2$, is denoted by $\widetilde{F}^{\mathrm{T}}(\xi,\eta)$. The family of non-standard bases $\widetilde{I}(\zeta,\chi)$ is given by

$$\widetilde{I}(\zeta,\chi) = \begin{pmatrix} I_3 & 0 \\ 0 & S_{\zeta,\chi} \end{pmatrix}, \quad \text{where} \quad S_{\zeta,\chi} = \begin{pmatrix} a & c & b \\ b & a & c \\ c & b & a \end{pmatrix}, \tag{4.6}$$

and

$$a(\zeta,\chi) = \frac{1}{3}(1 + e^{i\zeta} + e^{i\chi})\,, \tag{4.7}$$

$$b(\zeta,\chi) = \frac{1}{3}(1 + \omega^2 e^{i\zeta} + \omega e^{i\chi})\,, \tag{4.8}$$

$$c(\zeta,\chi) = \frac{1}{3}(1 + \omega e^{i\zeta} + \omega^2 e^{i\chi})\,. \tag{4.9}$$

Here, $S_{\zeta,\chi}$ is diagonal in the eigenbasis of the Heisenberg-Weyl operator X_3.

First, we show that the pair $\mathcal{P}_1 = \{I;\, \widetilde{F}^{\mathrm{T}}(\xi,\eta)\}$ is equivalent to $\{I;\, \widetilde{F}(\xi,\eta)\}$. To see this we multiply $\{I;\, \widetilde{F}\}$ with $\widetilde{F}^{\dagger}$, the adjoint of $\widetilde{F}$, from the left; this leaves us with $\{\widetilde{F}^{\dagger};\, I\}$. Then, by taking the complex conjugation we have $\{\widetilde{F}^{\mathrm{T}};\, I\}$, which after exchanging the order is indeed $\mathcal{P}_1$.

Next, we show that the matrix $\widetilde{F}(\xi,\eta)$ is equivalent to the Fourier family of Hadamard matrices $F(\xi,\eta)$ as defined in [88]. First we permute rows 2 and 5 of the matrix $\widetilde{F}(\xi,\eta)$, resulting in $\widetilde{F}'(\xi,\eta)$, the columns of which are no longer product vectors. Then we reorder the columns of $\widetilde{F}'$ such that columns $2,3,5$ and 6 become columns $6,2,3$ and 5, respectively, producing immediately the Fourier family $F(\xi,\eta)$. In some sense we have *derived* the Fourier family of Hadamard matrices from our construction of MU product bases, thereby "explaining" why this set depends on two real parameters. Since the transformations just described do not affect the standard basis, we have shown the equivalence of $\mathcal{P}_1$ with the pair $\{I;\, F(\xi,\eta)\}$.

Now we will show that the pair $\mathcal{P}_3 \equiv \{\widetilde{I}(\zeta,\chi);\, \widetilde{F}(\sigma,\tau)\}$ is also equivalent to $\mathcal{P}_1$. To see this, we transform the first basis $\widetilde{I}(\zeta,\chi)$ into the identity by multiplying it from the left with its inverse,

$$\begin{pmatrix} I_3 & 0 \\ 0 & S^{\dagger}_{\zeta,\chi} \end{pmatrix}, \tag{4.10}$$

where $S^{\dagger}_{\zeta,\chi}$ is the adjoint of $S_{\zeta,\chi}$, defined in (4.6), simultaneously mapping the matrix $\widetilde{F}(\sigma,\tau)$ (see Eq. (4.5)) to

$$\frac{1}{\sqrt{2}}\begin{pmatrix} F_3 & F_3 \\ S^{\dagger}_{\zeta,\chi}F_3 D & -S^{\dagger}_{\zeta,\chi}F_3 D \end{pmatrix}. \tag{4.11}$$

Since $S_{\zeta,\chi}$ is diagonal in the X_3 basis, the adjoint $S^{\dagger}_{\zeta,\chi}$ simply multiplies the columns of each matrix F_3 by phase factors. Writing $\sigma' = \sigma - \zeta$ and $\tau' = \tau - \chi$, we obtain the desired equivalence

$$\mathcal{P}_3 \sim \{I;\, \widetilde{F}(\sigma-\zeta,\tau-\chi)\} = \{I;\, \widetilde{F}(\sigma',\tau')\} \sim \mathcal{P}_1\,. \tag{4.12}$$

Finally, we show that $\mathcal{P}_2$ is equivalent to the pair $\{I;\, S_6\}$. We can express the pair as

$$\mathcal{P}_2 = \left\{ \begin{pmatrix} I_3 & 0 \\ 0 & -iH_y \end{pmatrix};\, \frac{1}{\sqrt{2}}\begin{pmatrix} F_3 & H_w \\ F_3 & -H_w \end{pmatrix} \right\}, \tag{4.13}$$

with matrices H_y and H_w defined in Eq. (3.17). To map the first matrix to the identity we multiply it with

$$\begin{pmatrix} I_3 & 0 \\ 0 & iH_y^{\dagger} \end{pmatrix} \tag{4.14}$$

from the left. The second matrix in $\mathcal{P}_2$ transforms to

$$\widetilde{S}_6 = \frac{1}{\sqrt{2}} \begin{pmatrix} F_3 & H_w \\ iH_y^\dagger F_3 & -iH_y^\dagger H_w \end{pmatrix}, \tag{4.15}$$

with

$$iH_y^\dagger F_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & \omega & \omega \\ \omega & 1 & \omega \\ \omega & \omega & 1 \end{pmatrix} \quad \text{and} \quad iH_y^\dagger H_w = -\frac{1}{\sqrt{3}} \begin{pmatrix} 1 & \omega^2 & \omega^2 \\ \omega^2 & 1 & \omega^2 \\ \omega^2 & \omega^2 & 1 \end{pmatrix}. \tag{4.16}$$

To transform $\widetilde{S}_6$ into the Hadamard matrix S_6 we perform a number of simple operations. First we exchange the second row of $\widetilde{S}_6$ with the third row as well as the fourth and fifth rows. Then we permute columns two with six, three with five, and four with five, followed by multiplying rows four and six with ω^2. These equivalence transformations indeed result in the matrix S_6, while their action on the identity is easily undone by column operations, thus establishing the equivalence relation

$$\mathcal{P}_2 \sim \{I;\, S_6\}. \tag{4.17}$$

This concludes our simplification of the list of MU product pairs. As with the Fourier family, we have "derived" the isolated matrix S_6 from a pair of MU product bases.

To summarise, the standard form for the MU product pairs listed in Eqs. (4.1)–(4.4) reduces to

$$\begin{aligned} \mathcal{P}_0 &\sim \{I;\, F(0,0)\}, \\ \mathcal{P}_1 \sim \mathcal{P}_3 &\sim \{I;\, F(\xi,\eta)\}, \\ \mathcal{P}_2 &\sim \{I;\, S_6\}, \end{aligned} \tag{4.18}$$

with $\mathcal{P}_1$ and $\mathcal{P}_3$ equivalent to a two-parameter family and $\mathcal{P}_2$ an isolated pair.

It is now straightforward to complete the proof of Theorem 4.0.1. Using computer-aided methods, it has been shown that the standard basis together with the isolated Hadamard S_6 *cannot* be extended to a triple of MU bases: there are 90 vectors MU to $\{I;\, S_6\}$ [17] but no two of them are orthogonal [18]. Thus, $\mathcal{P}_2$ cannot figure in a complete set of seven MU bases. Combining numerical calculations with rigorous error bounds [45], all pairs of MU bases involving members of the Fourier family[1] have been shown rigorously not to extend to quadruples of MU bases (cf. Section 2.5.2). These two results cover all cases given in (4.18), and hence all MU product pairs of Theorem 3.5.1. It follows that *no complete set of seven MU bases in* $d = 6$ *contains a pair of MU product bases*, i.e. Theorem 4.0.1.

We set out in the previous chapter with the modest goal to construct all MU product bases in dimension six. Using the resulting exhaustive list of MU product pairs, we have now been able to conclude that six of the seven MU bases required for a complete set in $\mathbb{C}^6$ must contain entangled states. To our knowledge, this is the strongest rigorous result concerning the structure of MU bases for $d = 6$. It considerably generalises the result that no pair of MU bases associated with the Heisenberg-Weyl operators of $\mathbb{C}^6$ gives rise to a complete set [34], at the same time providing an independent proof thereof. It is also stronger than a result given in [93], where the fixed entanglement content of a complete set in $d = 6$ has been used to show that no more than *three* of the seven hypothetical MU bases can be product bases. In addition, the current approach sheds some light on the particular character of the Fourier family of Hadamard matrices and the isolated matrix S_6, since these – and only these – matrices emerge naturally upon constructing all pairs of MU product bases in dimension six.

[1] In terms of our conventions, the result in [45] applies to the *transposed* Fourier family, i.e. directly to the pair $\mathcal{P}_1$ in Eq. (4.2).

Chapter 5

Unextendible product triples

In this chapter an *analytic* proof is given which shows that it is impossible to extend any triple of MU product bases in dimension six by a single MU vector, i.e. Theorem 3.6.1. While this result is already known, the final step of the proof in Section 3.6 relies on algebraic manipulations carried out by a computer [34]. In contrast, the method presented here follows from exploiting the structure of MU product bases in a novel fashion, and is one the strongest results obtained for MU bases in dimension six *without* recourse to computer algebra.

Only a few *analytic* results are known for sets of MU bases in composite dimensions such as $d = 6$ or $d = 10$ (see Section 2.4). The results we present in this chapter add to this list of known analytic results. We will start with a proof of the main theorem (Sec. 5.1), and then marginally improve this result by introducing MU product constellations (Sec. 5.2) and discuss the limitations of this approach. We summarise and discuss our results in Sec. 5.3.

5.1 Excluding MU product triples from a complete set of MU bases

We now present an *analytic* proof of Theorem 3.6.1, i.e. *No triple of MU product bases in dimension six can be extended by a single MU vector.* The starting point of our proof is the fact that, in dimension six, no more than two inequivalent triples of MU *product* bases exist, i.e. Theorem 3.5.2. Any product triple is equivalent, under specific unitary or anti-unitary transformations, to either

$$\begin{aligned} &\mathcal{T}_0 = \{|j_z, J_z\rangle;\ |j_x, J_x\rangle;\ |j_y, J_y\rangle\}\,, \\ \text{or}\quad &\mathcal{T}_1 = \{|j_z, J_z\rangle;\ |j_x, J_x\rangle;\ |0_y, J_y\rangle, |1_y, J_w\rangle\}\,, \end{aligned} \tag{5.1}$$

where $j = 0, 1$ and $J = 0, 1, 2$.

Due to Theorem 3.5.2, it is sufficient to show that no vector is MU to either of the triples $\mathcal{T}_0$ or $\mathcal{T}_1$; any other MU product triple can be transformed to one of these two triples using equivalence transformations.

A candidate state $|\psi\rangle \in \mathbb{C}^6$ is MU to the three product bases $\mathcal{T}_0$ if and only if the following 18 conditions hold,

$$|\langle j_a, J_a|\psi\rangle|^2 = \frac{1}{6}\,, \quad a = x, y, z\,; j = 0, 1\,; J = 0, 1, 2\,, \tag{5.2}$$

not all of which are independent. Similarly, the state $|\psi\rangle$ is mutually unbiased to the product triple $\mathcal{T}_1$ if and only if

$$|\langle j_z, J_z|\psi\rangle|^2 = |\langle j_x, J_x|\psi\rangle|^2 = |\langle 0_y, J_y|\psi\rangle|^2 = |\langle 1_y, J_w|\psi\rangle|^2 = \frac{1}{6}\,. \tag{5.3}$$

It will take us three steps to show that each of these two sets of equations is contradictory. In other words, there is *no* state $|\psi\rangle$ satisfying either the constraints (5.2) or (5.3).

Given a candidate state $|\psi\rangle \in \mathbb{C}^6$ we will derive (Step 1) that the smaller subsystem must reside in a totally mixed state which implies that the unknown state $|\psi\rangle \in \mathbb{C}^6$ is maximally entangled,

$$|\psi\rangle = \frac{1}{\sqrt{2}}\Big(|0_z\rangle \otimes |D\rangle + |1_z\rangle \otimes |D^\perp\rangle\Big)\,, \tag{5.4}$$

with any two orthogonal states $|D\rangle, |D^{\perp}\rangle \in \mathbb{C}^3$.

Then we will show (Step 2) that the states $|D\rangle$ and $|D^{\perp}\rangle$ are given by two states either of the basis $\mathcal{B}_y$ or of $\mathcal{B}_w$, displayed in Eqs. (3.17). Calling these states $|H\rangle$ and $|H^{\perp}\rangle$, a total of twelve candidates remains, namely

$$|\psi\rangle = \frac{1}{\sqrt{2}}\Big(|0_z\rangle \otimes |H\rangle + |1_z\rangle \otimes |H^{\perp}\rangle\Big) \,. \tag{5.5}$$

However, any state $|\psi\rangle$ of the form (5.5) will turn out to be incompatible with some MU conditions not used so far (Step 3).

Step 1: Fix the values of j and a in Eqs. (5.2). Summing over J leads to six equations

$$\sum_{J=0}^{2} |\langle j_a, J_a|\psi\rangle|^2 = \langle j_a| \Big[\mathrm{tr}_B|\psi\rangle\langle\psi|\Big] |j_a\rangle = \langle j_a|\rho_A|j_a\rangle = \frac{1}{2} \,, \tag{5.6}$$

which are sufficient to determine the components of the Bloch vector $\vec{n}$ of $\rho_A = (I_A + \vec{n}\cdot\vec{\sigma})/2$. Since the spin components are given by $\sigma_a = |0_a\rangle\langle 0_a| - |1_a\rangle\langle 1_a|$, one finds that

$$n_a \equiv \mathrm{tr}_A\big[\sigma_a \rho_A\big] = 0 \,, \quad a = x, y, z \,, \tag{5.7}$$

which means that the smaller subsystem must reside in the maximally mixed state,

$$\rho_A \equiv \mathrm{tr}_B|\psi\rangle\langle\psi| = \frac{1}{2} I_A \,. \tag{5.8}$$

Summing Eqs. (5.3) over J, with j and a fixed, results in the same six equations $\langle j_a|\rho_A|j_a\rangle = 1/2$, hence Eq. (5.8) holds in this case as well.

Next, the Schmidt decomposition of a state $|\psi\rangle \in \mathbb{C}^6$ reads

$$|\psi\rangle = \lambda_1 |c\rangle \otimes |C\rangle + \lambda_2 |c^{\perp}\rangle \otimes |C^{\perp}\rangle \tag{5.9}$$

where $\big\{|c\rangle, |c^{\perp}\rangle\big\}$ and $\big\{|C\rangle, |C^{\perp}\rangle, |C^{\perp\!\perp}\rangle\big\}$ are appropriately chosen orthonormal bases of the spaces $\mathbb{C}^2$ and $\mathbb{C}^3$ respectively, while $\lambda_{1,2}$ are two positive numbers satisfying $\lambda_1^2 + \lambda_2^2 = 1$. Eq. (5.8) implies that these coefficients must be equal so that $\lambda_1 = \lambda_2 = 1/\sqrt{2}$ follows. Consequently, we are free to identify the basis $\big\{|c\rangle, |c^{\perp}\rangle\big\}$ with the standard basis $\big\{|0_z\rangle, |1_z\rangle\big\}$ of $\mathbb{C}^2$, at the expense of using a different orthonormal basis $\big\{|D\rangle, |D^{\perp}\rangle, |D^{\perp\!\!\perp}\rangle\big\}$ of $\mathbb{C}^3$, unitarily equivalent to $\big\{|C\rangle, |C^{\perp}\rangle, |C^{\perp\!\!\perp}\rangle\big\}$. Thus, the candidates for states MU to three product bases must be maximally entangled ones,

$$|\psi\rangle = \frac{1}{\sqrt{2}}\Big(|0_z\rangle \otimes |D\rangle + |1_z\rangle \otimes |D^{\perp}\rangle\Big)\,. \tag{5.10}$$

This result agrees with a known result: if a complete set of seven MU bases in dimension six contains three MU product bases then all states of the remaining four MU bases are maximally entangled [93].

Step 2: Now consider the reduced density matrix for the larger subsystem (with label B),

$$\rho_B = \frac{1}{2}\big(|D\rangle\langle D| + |D^{\perp}\rangle\langle D^{\perp}|\big)\,, \tag{5.11}$$

which has eigenvalues $(1/2, 1/2, 0)$, in agreement with those of ρ_A in (5.8), except for a padded zero. The requirement that the state $|\psi\rangle$ be MU to the states $\big\{|j_z, J_z\rangle\big\}$ and $\big\{|j_x, J_x\rangle\big\}$, which appear in both triples, imposes restrictions on the states $|D\rangle$ and $|D^{\perp}\rangle$. Summing the conditions in (5.2) and (5.3) over all values of j while keeping J fixed, one obtains six further constraints now on the density matrix ρ_B,

$$\sum_{j=0}^{1} |\langle j_a, J_a|\psi\rangle|^2 = \langle J_a|\Big[\mathrm{tr}_A|\psi\rangle\langle\psi|\Big]|J_a\rangle \equiv \langle J_a|\rho_B|J_a\rangle = \frac{1}{3}\,, \tag{5.12}$$

where $J = 0, 1, 2$ and $a = x, z$, similar in spirit to Eqs. (5.6). However, these expectation values are *not* sufficient to reconstruct the reduced density matrix ρ_B. Nevertheless, one can draw the important conclusion that

$$\big|\langle J_a|D^{\perp\!\!\perp}\rangle\big|^2 = \frac{1}{3}\,, \quad J = 0, 1, 2, \quad a = x, z\,. \tag{5.13}$$

To see this, use the resolution of the identity in terms of the D-basis of $\mathbb{C}^3$ to rewrite (5.11) as

$$\rho_B = \frac{1}{2}\big(I_B - |D^{\perp\!\!\perp}\rangle\langle D^{\perp\!\!\perp}|\big) \tag{5.14}$$

and calculate its expectation value in the state $|J_a\rangle$.

Eqs. (5.13) tell us that the state $|D^{\perp\!\!\perp}\rangle$ is MU to the states of the MU bases $\mathcal{B}_x$ and $\mathcal{B}_z$ of $\mathbb{C}^3$. This leaves only a small number of possibilities for the state $|D^{\perp\!\!\perp}\rangle$: it must coincide with one of the six vectors $|J_y\rangle, |J_w\rangle, J = 0, 1, 2$, which form $\mathcal{B}_y$ and $\mathcal{B}_w$, since

– as shown in [18] – these are indeed the only states in $\mathbb{C}^3$ MU to the pair $\mathcal{B}_z$ and $\mathcal{B}_x$. Letting $|D^{\perp\!\!\perp}\rangle \equiv |H^{\perp\!\!\perp}\rangle$, where $|H^{\perp\!\!\perp}\rangle$ is any of the six states in $\mathcal{B}_y \cup \mathcal{B}_w$, the states $|D\rangle$ and $|D^{\perp}\rangle$ must be linear combinations of $|H\rangle$ and $|H^{\perp}\rangle$. After removing overall phase factors, we can thus write

$$\begin{aligned} |D\rangle &= \cos\tfrac{\vartheta}{2}\,|H\rangle + e^{i\phi}\sin\tfrac{\vartheta}{2}\,|H^{\perp}\rangle\,, \\ |D^{\perp}\rangle &= \sin\tfrac{\vartheta}{2}\,|H\rangle - e^{i\phi}\cos\tfrac{\vartheta}{2}\,|H^{\perp}\rangle\,, \end{aligned} \tag{5.15}$$

with two real parameters $\vartheta \in [0,\pi]$, and $\phi \in [0,2\pi)$. Projecting the candidate $|D\rangle$ given in (5.15) onto the states $|J_z\rangle, J = 0,1,2$, produces three constraints on the free parameters:

$$\big|\langle J_z|D\rangle\big|^2 \equiv \big|\langle J_z|\big(\cos\frac{\vartheta}{2}\,|H\rangle + e^{i\phi}\sin\frac{\vartheta}{2}\,|H^{\perp}\rangle\big)\big|^2 = \frac{1}{3}\,. \tag{5.16}$$

Using $\big|\langle J_z|H\rangle\big|^2 = \big|\langle J_z|H^{\perp}\rangle\big|^2 = 1/3$, this equation leads to the conditions

$$\sin\frac{\vartheta}{2}\,\cos\frac{\vartheta}{2}\,\Big(e^{i\phi}\langle H|J_z\rangle\langle J_z|H^{\perp}\rangle + \text{c.c}\Big) = \frac{1}{3}\sin\vartheta\,\cos(\phi+\mu_J) = 0\,, \tag{5.17}$$

where the relation $\langle H|J_z\rangle\langle J_z|H^{\perp}\rangle \equiv (1/3)\,e^{i\mu_J}$ defines the angles $\mu_J \in [0,2\pi), J = 0,1,2$. However, the states $|H\rangle$ and $|H^{\perp}\rangle$ are orthogonal, which implies that

$$0 = \langle H|H^{\perp}\rangle = \sum_{J=0}^{2}\langle H|J_z\rangle\langle J_z|H^{\perp}\rangle = \frac{1}{3}\sum_{J=0}^{2} e^{i\mu_J}\,, \tag{5.18}$$

forcing

$$\mu_J = \mu + \frac{2\pi}{3}J\,, \quad J = 0,1,2\,, \tag{5.19}$$

with some constant $\mu \in [0,2\pi)$. Therefore, Eqs. (5.17) require either $\sin\vartheta \equiv 0$ or

$$\cos(\phi + \mu + \frac{2\pi}{3}J) = 0,\; J = 0,1,2\,. \tag{5.20}$$

Since the zeros of the cosine function occur at intervals of length π (not $2\pi/3$), we conclude that $\vartheta/2 \in \{0,\pi/2\}$ are the only values allowed in (5.15). An entirely analogous argument leads to the same conclusion if we consider the state $|D^{\perp}\rangle$ defined in (5.15) instead of $|D\rangle$.

Thus, we have shown that there are only two cases in which the requirements of (5.2) or (5.3) are satisfied: we must have either

$$|D\rangle = |H\rangle \quad \text{and} \quad |D^{\perp}\rangle = -e^{i\phi}|H^{\perp}\rangle\,, \tag{5.21}$$

or

$$|D\rangle = e^{i\phi}|H^{\perp}\rangle \quad \text{and} \quad |D^{\perp}\rangle = |H\rangle\,. \tag{5.22}$$

In both cases, the phase factors may be absorbed into the definition of the state $|H^{\perp}\rangle$, which leaves us with two possible candidates being MU to the three product bases in $\mathcal{T}_0$ or $\mathcal{T}_1$, namely

$$|\psi\rangle = \frac{1}{\sqrt{2}}\Big(|0_z\rangle \otimes |H\rangle + |1_z\rangle \otimes |H^{\perp}\rangle\Big)\,, \tag{5.23}$$

and the state obtained from swapping $|H\rangle$ with $|H^{\perp}\rangle$. Consequently, the requirement of the state $|D^{\perp\!\perp}\rangle$ to be a member of $\mathcal{B}_y$ or $\mathcal{B}_w$ implies that the states $|D\rangle$ and $|D^{\perp}\rangle$ must coincide with the two other members of the same basis. Overall, we have indeed reduced the possible states mutually unbiased to $\mathcal{T}_0$ or $\mathcal{T}_1$ to twelve entangled states listed in Eq. (5.5).

Step 3: Finally, we show that states $|\psi\rangle$ of the form (5.23) are not MU to the states $|1_x, J_x\rangle$, $J = 0, 1, 2$, which are present in both product triples, $\mathcal{T}_0$ and $\mathcal{T}_1$. The mechanics to produce this contradiction is similar to the one given at the end of Step 2.

To begin, let us consider the state $|\psi\rangle$ in (5.23): the conditions

$$\frac{1}{2}\,\Big|\langle 1_x, J_x|\Big(|0_z\rangle \otimes |H\rangle + |1_z\rangle \otimes |H^{\perp}\rangle\Big)\rangle\Big|^2 = \frac{1}{6} \tag{5.24}$$

lead to

$$\langle H|J_x\rangle\langle J_x|H^{\perp}\rangle + \langle H^{\perp}|J_x\rangle\langle J_x|H\rangle = 0\,. \tag{5.25}$$

Upon writing $\langle H|J_x\rangle\langle J_x|H^{\perp}\rangle \equiv (1/3)\,e^{i\nu_J}$, one obtains

$$\cos\left(\nu + \frac{2\pi}{3}J\right) = 0\,, \quad J = 0, 1, 2\,, \tag{5.26}$$

where we have used the fact that the orthogonality of the states $|H\rangle$ and $|H^{\perp}\rangle$ restricts the values of the phases ν_J in analogy to Eqs. (5.19). However, the three equations in (5.26) cannot hold simultaneously, and the state $|\psi\rangle$ in (5.23) is found *not* to be MU to the given three product bases. This completes the proof that there is not a single state mutually unbiased to the triple $\mathcal{T}_0$ or $\mathcal{T}_1$.

5.2 An unextendible MU product constellation

We now marginally strengthen Theorem 3.6.1 by considering the constellation $\{5,5,4\}_6^{\otimes}$ which consists of two product bases (five orthonormal rays in $\mathbb{C}^6$ determine a unique sixth state so that it is not listed in this notation), and a set $\mathcal{S}$ of four orthogonal product states.

Theorem 5.2.1. *The product constellation* $\{5,5,4\}_6^{\otimes}$ *cannot be part of a complete set of seven MU bases.*

This result is an immediate consequence of the following lemma, the proof of which will form the main part of this section.

Lemma 5.2.2. *The product constellation* $\{5,5,4\}_6^{\otimes}$ *extends to a triple of MU bases only by adding* product *states.*

If the product constellation $\{5,5,4\}_6^{\otimes}$ was part of a complete set of seven MU bases, Lemma 5.2.2 would imply that the complete set must contain a *triple* of MU product bases, contradicting Theorem 3.6.1.

To prove Lemma 5.2.2, we need the complete list of pairs of MU product bases obtained in Theorem 3.5.1, i.e.

$$\begin{aligned}
\mathcal{P}_0 &= \{|j_z, J_z\rangle;\ |j_x, J_x\rangle\}\,,\\
\mathcal{P}_1 &= \{|j_z, J_z\rangle;\ |0_x, J_x\rangle, |1_x, \hat{R}_{\xi,\eta} J_x\rangle\}\,,\\
\mathcal{P}_2 &= \{|0_z, J_z\rangle, |1_z, J_y\rangle;\ |0_x, J_x\rangle, |1_x, J_w\rangle\}\,,\\
\mathcal{P}_3 &= \{|0_z, J_z\rangle, |1_z, \hat{S}_{\zeta,\chi} J_z\rangle;\ |j_x, 0_x\rangle, |\hat{r}_\sigma j_x, 1_x\rangle, |\hat{r}_\tau j_x, 2_x\rangle\}\,.
\end{aligned} \tag{5.27}$$

The four product states in $\mathcal{S}$ must be MU to one of these pairs. However, we can exclude the pairs $\mathcal{P}_2$ and $\mathcal{P}_3$ since no product state can be MU to either pair, as follows from Theorem 3.3.2 given in Sec. 3.3. The pair $\mathcal{P}_2$ contains a complete set of four MU bases for the space $\mathbb{C}^3$ which means there is no other product state MU to $\mathcal{P}_2$. Similarly, no state in $\mathbb{C}^2$ is MU to the bases $\{|j_z\rangle\}$, $\{|j_x\rangle\}$ and $\{|\hat{r}_\sigma j_x\rangle\}$, ($\hat{r}_\sigma \neq \hat{I}$), and therefore no product state MU to $\mathcal{P}_3$ exists. Thus, the two MU bases of any MU product constellation of the form $\{5,5,4\}_6^{\otimes}$ are given by either of the pairs $\mathcal{P}_0$ or $\mathcal{P}_1$.

We now use Theorems 3.3.2 and 3.5.1 to limit the form of the four states which make up the set $\mathcal{S}$. Since there are only three MU bases in $\mathbb{C}^2$, the first factor of each of the four states in $\mathcal{S}$ must be either $|0_y\rangle$ or $|1_y\rangle$, giving rise to only two possibilities, either

$$\mathcal{S}_1 = \{|0_y, A\rangle, |0_y, A^{\perp}\rangle, |0_y, A^{\perp\!\!\perp}\rangle, |1_y, B\rangle\} \tag{5.28}$$

or

$$\mathcal{S}_2 = \{|0_y, A\rangle, |0_y, A^{\perp}\rangle, |1_y, B\rangle, |1_y, B^{\perp}\rangle\}, \tag{5.29}$$

where $\{|A\rangle, |A^{\perp}\rangle, |A^{\perp\!\!\perp}\rangle\}$ and $\{|B\rangle, |B^{\perp}\rangle, |B^{\perp\!\!\perp}\rangle\}$ denote two orthonormal bases in $\mathbb{C}^3$. The crucial point here is to observe that both $|0_y\rangle$ and $|1_y\rangle$ can occur at most three times as a factor – otherwise the states in $\mathcal{S}$ could not be orthogonal. Each state of the set $\mathcal{S}$ must be MU to all states of either $\mathcal{P}_0$ or $\mathcal{P}_1$, which implies that any one of the six states $|A\rangle, \ldots, |B^{\perp\!\!\perp}\rangle$, occurring in (5.28) or (5.29) must be MU to the bases $\mathcal{B}_z$ and $\mathcal{B}_x$. This requirement limits the states to members of the bases $\mathcal{B}_y$ or $\mathcal{B}_w$.

The states $|1_y, B^{\perp}\rangle$ and $|1_y, B^{\perp\!\!\perp}\rangle$ are orthogonal to the quadruple (5.28), as are their linear combinations,

$$|\psi_1\rangle = \alpha|1_y, B^{\perp}\rangle + \beta|1_y, B^{\perp\!\!\perp}\rangle \equiv |1_y\rangle \otimes (\alpha|B^{\perp}\rangle + \beta|B^{\perp\!\!\perp}\rangle), \tag{5.30}$$

with $|\alpha|^2 + |\beta|^2 = 1$. Hence, adding any two orthogonal states from this family to the set $\mathcal{S}_1$ in (5.28) produces a MU *product* basis.

Any orthonormal state extending the set $\mathcal{S}_2$ in (5.29) can be written as

$$|\psi_2\rangle = \alpha|0_y, A^{\perp\!\!\perp}\rangle + \beta|1_y, B^{\perp\!\!\perp}\rangle, \tag{5.31}$$

which is *entangled* unless $|A^{\perp\!\!\perp}\rangle = |B^{\perp\!\!\perp}\rangle$ or one of the constants α and β is zero. We now show that the state $|\psi_2\rangle$ cannot be entangled if it is to satisfy the MU conditions

$$|\langle 0_z, J_z|\psi_2\rangle|^2 = \frac{1}{6}, \qquad J = 0, 1, 2. \tag{5.32}$$

Write $|A^{\perp\!\!\perp}\rangle = (\omega_0|0_z\rangle + \omega_1|1_z\rangle + \omega_2|2_z\rangle)/\sqrt{3}$ and $|B^{\perp\!\!\perp}\rangle = (\omega_0'|0_z\rangle + \omega_1'|1_z\rangle + \omega_2'|2_z\rangle)/\sqrt{3}$, where $\omega_0 = \omega_0' = 1$ and each of the four coefficients $\omega_1, \ldots, \omega_2'$ is a third root of unity such that the states $|A^{\perp\!\!\!\perp}\rangle$ and $|B^{\perp\!\!\!\perp}\rangle$ coincide with any two different states of the bases $\mathcal{B}_y$ and $\mathcal{B}_w$. Then, the MU conditions in (5.32) turn into

$$\alpha\beta^*\langle J_z|A^{\perp\!\!\!\perp}\rangle\langle B^{\perp\!\!\!\perp}|J_z\rangle + \alpha^*\beta\langle J_z|B^{\perp\!\!\!\perp}\rangle\langle A^{\perp\!\!\!\perp}|J_z\rangle = 0\,, \quad J = 0,1,2\,, \tag{5.33}$$

or explicitly,

$$\alpha\beta^*\omega_J\omega_J^{*\prime} + \alpha^*\beta\omega_J^*\omega'_J = 0\,, \quad J = 0,1,2\,. \tag{5.34}$$

For $J = 0$, we find the relation

$$\alpha\beta^* + \alpha^*\beta = 0\,, \tag{5.35}$$

which, when used in (5.34), leads to

$$\alpha\beta^*(\omega_J\omega^{*\prime}{}_J - \omega_J^*\omega'_J) = 0\,, \quad J = 1,2\,. \tag{5.36}$$

However, these constraints on the phase factors cannot be satisfied by any allowed choice of the pair of states $|A^{\perp\!\!\!\perp}\rangle$ and $|B^{\perp\!\!\!\perp}\rangle$ with $|A^{\perp\!\!\!\perp}\rangle \neq |B^{\perp\!\!\!\perp}\rangle$. Thus, either α or β must equal zero, and we conclude that $|\psi_2\rangle$ is a product state. This completes the proof of Lemma 5.2.2.

5.3 Summary

The main result of this chapter is an *analytical* proof that no vector is MU to any triple of MU product bases, i.e. Theorem 3.6.1. Our approach exploits the structure of MU product bases in a novel fashion, and it is entirely independent of any computer algebraic methods. Thus, we consider it to be a worthy addition to the few existing analytic results on MU bases in dimension six.

Results stronger than Theorem 3.6.1 are known which exclude a wider class of MU bases from complete sets. For example, the proof that the Heisenberg-Weyl pair of bases $\{|j_z, J_z\rangle\}$ and $\{|j_x, J_x\rangle\}$ is MU to at most one further basis [34] and the numerical search for bases mutually unbiased to the Fourier family [45]. However, these both rely on a computer in one way or another.

It is worth recalling that a hypothetical complete set of MU bases in dimension six will contain at most *one* product basis as shown in the previous chapter. While this is a stronger statement than the one obtained here, the proof depends on a numerical search with rigorous error bounds [45].

A recent analytic result [62] employs combinatorial and Fourier analytic arguments to prove that no complete set of MU bases in dimension six will contain both the standard and Fourier basis. As a consequence, no complete set of MU bases will contain triples of MU product bases. Whilst this is also a consequence of Theorem 3.6.1, the result presented here is different since we have shown the impossibility to extend a product triple by a *single* MU vector. The result in [62] does not seem to forbid such an extension.

In order to strengthen Theorem 3.6.1 we also considered a MU product *constellation* that is slightly smaller than MU product triples. The resulting Theorem 5.2.1 states that the product constellation $\{5,5,4\}_6^{\otimes}$ cannot be part of a complete set of seven MU bases. Its derivation relies on an enumeration of *all* pairs of MU product bases in dimension six which was given in Section 3.5.1.

To make any stronger statements regarding product constellations seems to be surprisingly difficult. For example, we are not able to show whether a complete set of seven MU bases contains the MU constellation $\{5,4,4\}_6^{\otimes}$, consisting of one MU product basis and two sets of four orthogonal MU product states. The main difficulty is that the proof of Theorem 5.2.1 relies on Theorem 3.3.2 which does not apply to the constellation $\{5,4,4\}_6^{\otimes}$.

Chapter 6

Isolated complex Hadamard matrices

In this chapter a new construction of complex Hadamard matrices of composite order $d = pq$, with primes p, q, is presented which is based on pairs of MU bases containing only product states. For product dimensions $d < 100$, we illustrate the method by deriving many previously unknown complex Hadamard matrices. We obtain at least 12 new *isolated* matrices of Butson-type, with orders ranging from 9 to 91.

The method we use to construct Hadamard matrices originates from earlier studies on *pairs* of MU *product* bases in dimension six presented in Chapters 3 and 4. Generalising this method from $d = 2 \times 3$ to composite dimensions $d = pq$, we establish a general construction method resulting in previously undiscovered complex Hadamard matrices.

The chapter is organised as follows: In Section 6.1 we summarise those properties of complex Hadamard matrices which we will use in later sections. Section 6.2 includes our first main result, Theorem 6.2.1, which describes a general construction for complex Hadamard matrices of size $d = pq$. In Section 6.3 we apply Theorem 6.2.1 to find new complex Hadamard matrices for $d \leq 15$. We briefly touch upon higher dimensions as well as potential generalisations of the construction in Section 6.4. Section 6.5 contains a summary of our results.

6.1 Complex Hadamard matrices refresher

As we have already discussed (see Section 2.2), MU bases in a finite-dimensional Hilbert space $\mathbb{C}^d$ are closely related to complex Hadamard matrices of order d. Given a set of $(r+1)$ MU bases in standard form $\{\mathcal{I}, \mathcal{B}_1, \ldots \mathcal{B}_r\}$, where $\mathcal{I}$ is the standard basis, the bases $\mathcal{B}_1, \ldots, \mathcal{B}_r$ are represented by $(d \times d)$ complex Hadamard matrices, $H_1, \ldots, H_r$. Here the vectors of each basis form the columns of a matrix. Since these matrices are MU to the identity matrix, their matrix elements have modulus $1/\sqrt{d}$.

It is often the case that a single Hadamard matrix is contained in a subset of a larger continuous family of complex Hadamard matrices. The *defect* $d(H)$ of a Hadamard matrix H, defined in [88], provides an upper bound on the dimensionality of any set of Hadamard matrices stemming from H. If a dephased Hadamard matrix has a defect of zero then the matrix is called *isolated*, expressing the fact that all complex Hadamard matrices in a neighbourhood of H are equivalent. To calculate the defect of H, we multiply all elements of the Hadamard matrix with independent phase factors, i.e. $H_{ij} \to e^{a_{ij}} H_{ij}$ for $i, j = 2 \ldots d$, and solve the set of equations, to first order, which are imposed by the unitarity condition (see [10] for an explicit example). For all but the smallest dimensions d or special cases, it seems imperative to use a computer program in order to determine the defect; the software we have used is MATLAB [1]. The defect provides only a weak upper bound on the dimensionality of a Hadamard family; higher-order solutions of the unitarity conditions often lead to stronger bounds [8].

6.1.1 Known constructions in composite dimensions

There are many known constructions of complex Hadamard matrices (e.g. [21]), some of which apply only to specific dimensions. We briefly review two constructions of (affine) complex Hadamard matrices based on the tensor product of smaller matrices following [86].

Theorem 6.1.1. (Hosoya-Suzuki [40]) *Let $M_1, M_2, \ldots, M_v$ be $k \times k$, $N_1, N_2, \ldots, N_k$ be $v \times v$ complex Hadamard matrices. Then the generalised tensor product matrix, denoted* *by $Q = (M_1, M_2, \ldots, M_v) \otimes (N_1, N_2, \ldots, N_k)$, whose (i, j)th block is given by the matrix $Q_{ij} = diag([M_1]_{ij}, [M_2]_{ij}, \ldots, [M_v]_{ij})N_j$, is a complex Hadamard matrix of order vk.*

By using a simpler version of this tensor product structure, these matrices can be *parameterised*, i.e. embedded in larger families of Hadamard matrices.

Corollary 6.1.2. (Diţă [28]) *Let $M = (m_{ij})$ be a $k \times k$ and $N_1, N_2, \ldots, N_k$ be $v \times v$ dephased complex Hadamard matrices with m and $n_1, n_2, \ldots, n_k$ free parameters, respectively, and let $D_2, \ldots, D_k$ be $v \times v$ unitary diagonal matrices each containing $(v - 1)$ free parameters. Then the block matrix*

$$Q = \begin{pmatrix} m_{11}N_1 & m_{12}D_2N_2 & \ldots & m_{1k}D_kN_k \\ \vdots & & & \\ m_{k1}N_1 & m_{k2}D_2N_2 & \ldots & m_{kk}D_kN_k \end{pmatrix}, \tag{6.1}$$

is a complex Hadamard matrix of order vk with $m + \sum_{i=1}^{k} n_i + (k - 1)(v - 1)$ free parameters.

Any matrix which can be derived from Corollary 6.1.2 is called a *Diţă-type* complex Hadamard matrix.

6.1.2 Butson-type complex Hadamard matrices

We finally recall a special class of Hadamard matrices called *Butson-Hadamard* matrices.

Definition 6.1.3. *A complex Hadamard matrix of order d is a Butson-Hadamard matrix $BH(d, r)$ if its elements are r^{th} roots of unity, apart from a factor $1/\sqrt{d}$.*

It is straightforward to show that a Hadamard matrix is (equivalent to one) of Butson-type $BH(d, r)$: once dephased, all its matrix elements must be r^{th} roots of unity.

The simplest examples of Butson-type matrices occur when $r = 2$; in this case the matrices $BH(d, 2)$ are the set of $(d \times d)$ *real* Hadamard matrices. The existence of $BH(d, r)$ matrices for arbitrary values of d and r is still an open problem; it remains unknown, for example, if real Hadamard matrices of the form $B(4n, 2)$ exist for all integers n. A summary of existing Butson-Hadamard matrices with fourth and sixth roots of unity can be found in [86] and the known $BH(d, r)$ matrices for $d \leq 16$ are given in [21]. There are also several existence theorems for $BH(d, r)$ matrices, e.g.

Theorem 6.1.4. (Butson [24]) *When p is prime, a $BH(2p, p)$ matrix can be constructed.*

For $p = 3$, the matrix $BH(6, 3)$ turns out to be the isolated matrix S_6, which was also found independently in [65, 89]. We have derived the matrices $B_{10} \in BH(10, 5)$ and $B_{14} \in BH(14, 7)$ following Butson's method (see Appendix D) since they will be important in the present context and seem to be unavailable in the literature.

Butson-Hadamard matrices will appear in Sections 6.3 and 6.4, where we derive previously unknown examples of complex Hadamard matrices of orders up to 91. Most of these examples cannot be constructed from Theorem 6.1.4.

6.2 Complex Hadamard matrices from pairs of MU product bases

The following theorem shows how to construct a complex Hadamard matrix of order $d = pq$ where p and q are both prime, using sets of MU bases in dimensions p and q.

Theorem 6.2.1. *Suppose that $K_0, \dots, K_{p-1}$ and $L_0, \dots, L_{p-1}$ are unitary matrices of order q such that $K_m^\dagger L_n$ are complex Hadamard matrices for all $m, n = 0, \dots, p-1$, i.e. K_m is MU to L_n, and let $\alpha_{ij}/\sqrt{p}$ be the (i, j)th element of a complex Hadamard matrix M of order p, with $|\alpha_{ij}| = 1$. Then the block matrix H_{pq} given by*

$$H_{pq} = \frac{1}{\sqrt{p}} \begin{pmatrix} \alpha_{11} K_0^\dagger L_0 & \alpha_{12} K_0^\dagger L_1 & \dots & \alpha_{1p} K_0^\dagger L_{p-1} \\ \alpha_{21} K_1^\dagger L_0 & \alpha_{22} K_1^\dagger L_1 & \dots & \alpha_{2p} K_1^\dagger L_{p-1} \\ \alpha_{31} K_2^\dagger L_0 & \alpha_{32} K_2^\dagger L_1 & \dots & \alpha_{3p} K_2^\dagger L_{p-1} \\ \vdots & & & \\ \alpha_{p1} K_{p-1}^\dagger L_0 & \alpha_{p2} K_{p-1}^\dagger L_1 & \dots & \alpha_{pp} K_{p-1}^\dagger L_{p-1} \end{pmatrix} \tag{6.2}$$

is a complex Hadamard matrix of order pq.

The theorem follows easily from factorising the matrix H_{pq} such that $H_{pq} = B_1^\dagger B_2$, where

$$B_1 = \begin{pmatrix} K_0 & 0 & \dots & 0 \\ 0 & K_1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & K_{p-1} \end{pmatrix} \tag{6.3}$$

and

$$B_2 = \begin{pmatrix} \alpha_{11}L_0 & \alpha_{12}L_1 & \dots & \alpha_{1p}L_{p-1} \\ \alpha_{21}L_0 & \alpha_{22}L_1 & \dots & \alpha_{2p}L_{p-1} \\ \vdots & \vdots & & \vdots \\ \alpha_{p1}L_0 & \alpha_{p2}L_1 & \dots & \alpha_{pp}L_{p-1} \end{pmatrix}. \tag{6.4}$$

The column vectors of the unitary matrices B_1 and B_2 form a pair of MU bases since the block matrices K_m are MU to L_n, i.e. $K_m^\dagger L_n$ are complex Hadamard matrices for all $m, n = 0, \dots, p-1$. Thus, by mapping B_1 to the identity matrix using the unitary transformation $B_1^\dagger$, the matrix B_2 is simultaneously mapped to $B_1^\dagger B_2 = H_{pq}$, which is a complex Hadamard matrix. This completes the proof of Theorem 6.2.1.

In fact, the matrices B_1 and B_2 correspond to a pair of MU *product* bases where the columns of B_1 and B_2 form the vectors of each basis. We can write the pair of matrices B_1 and B_2 as the orthonormal bases

$$\mathcal{B}_1 = \Big\{|0_z\rangle \otimes \mathcal{K}_0,\, |1_z\rangle \otimes \mathcal{K}_1,\, \dots,\, |(p-1)_z\rangle \otimes \mathcal{K}_{p-1}\Big\} \tag{6.5}$$

and

$$\mathcal{B}_2 = \Big\{|0_a\rangle \otimes \mathcal{L}_0,\, |1_a\rangle \otimes \mathcal{L}_1,\, \dots,\, |(p-1)_a\rangle \otimes \mathcal{L}_{p-1}\Big\}, \tag{6.6}$$

respectively, where $|m_z\rangle \otimes \mathcal{K}_m$ denotes the tensor product of a state $|m_z\rangle$ from the standard basis of $\mathbb{C}^p$ with all states from a basis $\mathcal{K}_m$ of the space $\mathbb{C}^q$ corresponding to the matrix K_m. Similarly, $|n_a\rangle \otimes \mathcal{L}_n$ is defined such that $|n_a\rangle$ is a state in $\mathbb{C}^p$ corresponding to the nth column vector of the $(p \times p)$ Hadamard matrix M, and $\mathcal{L}_n$ is a basis of $\mathbb{C}^q$ corresponding to the matrix L_n. Thus, by mapping $\mathcal{B}_1$ to the standard basis, the columns of the second basis $\mathcal{B}_2$ form the complex Hadamard matrix H_{pq}.

To simplify the matrix H_{pq} we perform equivalence transformations on the pair of MU bases $\{\mathcal{B}_1, \mathcal{B}_2\}$ such that $\mathcal{K}_0$ and $\mathcal{L}_0$ are mapped to the standard and Fourier basis of $\mathbb{C}^q$ respectively, and the orthonormal basis $\{|0_a\rangle, \dots, |(p-1)_a\rangle\}$ is mapped to the Fourier basis of $\mathbb{C}^p$, i.e. $K_0 \equiv I_q$, $L_0 \equiv F_q$ and $M \equiv F_p$, with I_q the $(q \times q)$ identity matrix, and F_p, F_q, being the Fourier matrices of order p and q respectively. Since B_1 is MU to B_2, the set $\{I_q, K_1, K_2, \dots, K_{p-1}\}$ is MU to $\{F_q, L_1, \dots, L_{p-1}\}$, and as a consequence, $L_1, \dots, L_{p-1}$ are complex Hadamard matrices. We will continue to use the simplification $M \equiv F_p$, $K_0 \equiv I_q$ and $L_0 \equiv F_q$ throughout.

In the trivial case of $K_1 = \dots = K_{p-1} = I_q$, one can choose each matrix L_n to be a $(q-1)$-parameter family DF_q where $D = \text{diag}(1, e^{a_1^n}, \dots, e^{a_{q-1}^n})$ for each $n > 0$. In this case, H_{pq} is a $(p-1)(q-1)$-parameter family of complex Hadamard matrices.

In the following section we will show that for certain choices of the $(q \times q)$ matrices $K_1, \dots, K_{p-1}, L_1, \dots, L_{p-1}$, the matrix H_{pq} given in Theorem 6.2.1 supplies new examples of Hadamard matrices. Most of the matrices we find will be isolated, which is sufficient to confirm that Theorem 6.2.1 produces matrices not of Diţă-type: every Diţă-type matrix is embedded within a family depending on at least $(k-1)(v-1)$ free parameters, with $k, v > 1$.

6.3 Examples: $d \leq 15$

We will now use the construction given in Theorem 6.2.1 to find complex Hadamard matrices of composite dimensions $d = pq$, with prime numbers $p \leq q$. In this section, we limit ourselves to matrices of order $d \leq 15$ with $p \leq q$. Larger dimensions and possible generalisations of the construction will be considered briefly in Sec. 6.4.

6.3.1 Dimension four

In dimension four, all inequivalent complex Hadamard matrices are given by the one-parameter family $F_4(a)$, $a \in [0, \pi]$ which can be found in [19, 35]. We re-derive this family from Theorem 6.2.1 using the block matrix,

$$H_4 = \frac{1}{\sqrt{2}} \begin{pmatrix} F_2 & L_1 \\ K_1^\dagger F_2 & -K_1^\dagger L_1 \end{pmatrix}, \tag{6.7}$$

where

$$F_2 \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{6.8}$$

is the (2×2) Fourier matrix and L_1, K_1 are specific unitary matrices of order two; to apply Theorem 6.2.1 it is necessary that the set $\{I_2, K_1\}$ is MU to $\{F_2, L_1\}$.

If K_1 is chosen as the identity, then L_1 can take the form

$$L_1(a) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ e^{ia} & -e^{ia} \end{pmatrix}, \tag{6.9}$$

where the column vectors of L_1 are indeed MU to the standard basis; an overall phase factor has been removed using equivalence transformations. Thus, H_4 turns into a one-parameter family of complex Hadamard matrices,

$$H_4(a) = \frac{1}{\sqrt{2}} \begin{pmatrix} F_2 & L_1(a) \\ F_2 & -L_1(a) \end{pmatrix}. \tag{6.10}$$

By permuting rows it is easily shown that $H_4(a)$ is equivalent to the one-parameter Fourier family $F_4(a)$. One can exchange K_1 with L_1 but the resulting family is still equivalent to $F_4(a)$; no other choices are possible. Note that in the four-dimensional case, $F_4(a)$ is equivalent to the transposed Fourier family $(F_4(a))^T$, a relation that does not always hold for larger composite dimensions.

6.3.2 Dimension six

In Chapter 4, pairs of MU product bases of the form $\mathcal{B}_1 = \{|0_z\rangle \otimes \mathcal{K}_0, |1_z\rangle \otimes \mathcal{K}_1\}$ and $\mathcal{B}_2 = \{|0_x\rangle \otimes \mathcal{L}_0, |1_x\rangle \otimes \mathcal{L}_1\}$ were shown to give rise to the transposed Fourier family of complex Hadamard matrices and the isolated matrix $S_6 \in BH(6,3)$. Here we rederive this result on the basis of Theorem 6.2.1 where we start with the following (6×6)

matrix

$$H_6 = \frac{1}{\sqrt{2}} \begin{pmatrix} F_3 & L_1 \\ K_1^\dagger F_3 & -K_1^\dagger L_1 \end{pmatrix}, \tag{6.11}$$

where F_3 is the (3×3) Fourier matrix defined in Eq. (3.16) and K_1, L_1 are unitary matrices of order three. The bases $\mathcal{B}_1$ and $\mathcal{B}_2$ will be MU if the pair $\{I_3, K_1\}$ is MU to the pair $\{F_3, L_1\}$. A proof given in Appendix C limits the possible choices for the matrices K_1 and L_1 to just three: (i) $K_1 = I_3$; (ii) $L_1 = F_3$; and (iii) all four matrices are pairwise MU.

If $K_1 = I_3$, the most general set of matrices satisfying the MU conditions is a two-parameter set,

$$L_1(a,b) = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ e^{ia} & \omega e^{ia} & \omega^2 e^{ia} \\ e^{ib} & \omega^2 e^{ib} & \omega e^{ib} \end{pmatrix}. \tag{6.12}$$

Thus, H_6 becomes a two-parameter family of complex Hadamard matrices which is equivalent to the transposed Fourier family $(F_6^{(2)})^T$.

If all four matrices I_3, F_3, K_1 and L_1 are MU then $K_1 = H_y$ and $L_1 = H_w$ or vice versa, with H_y and H_w defined in Eq. (3.17). Here, $\{I_3, F_3, H_y, H_w\}$ is the complete set of MU bases in $\mathbb{C}^3$. The complex Hadamard matrix H_6 in (6.11) associated with $K_1 = H_y$ and $L_1 = H_w$ is equivalent to S_6, the only known isolated complex Hadamard matrix of order six.

Thus, we have indeed constructed the transposed Fourier family of complex Hadamard matrices and the isolated matrix S_6 from Theorem 6.2.1. There are many more Hadamard matrices of order six, including three- and four-parameter families, as described in Section 2.2, but none of these can be derived from Theorem 6.2.1.

6.3.3 Dimension nine

The online catalogue [21] lists three types of complex Hadamard matrices of order nine: the four-parameter Fourier family $F_9^{(4)}$, the isolated matrix N_9 [9], and the matrix B_9 which has a defect of two [9]. Three Butson-Hadamard matrices are among these, namely $F_3 \otimes F_3 \in BH(9,3)$, $F_9 \in BH(9,9)$ and $B_9 \in BH(9,10)$. Theorem 6.2.1 allows us to identify an additional isolated Butson-Hadamard matrix of the form $BH(9,6)$.

The matrix in Eq. (6.2), for $d = 9$, has the structure

$$H_9 = \frac{1}{\sqrt{3}} \begin{pmatrix} F_3 & L_1 & L_2 \\ K_1^\dagger F_3 & \omega K_1^\dagger L_1 & \omega^2 K_1^\dagger L_2 \\ K_2^\dagger F_3 & \omega^2 K_2^\dagger L_1 & \omega K_2^\dagger L_2 \end{pmatrix}, \tag{6.13}$$

where $\omega = e^{2\pi i/3}$ is a third root of unity, and the matrices I_3 and F_3 are the (3×3) identity and Fourier matrix, respectively. The (3×3) matrices K_1, K_2, L_1 and L_2 must be chosen such that the set $\{I_3, K_1, K_2\}$ is MU to $\{F_3, L_1, L_2\}$.

In the six-dimensional case (cf. Sec 6.3.2), the choice of pairs $\{I, K_1\}$ and $\{F_3, L_1\}$ was limited to either two matrices having identical columns (up to column permutations) or all four matrices being MU. Similarly, the choices for the triples $\{I_3, K_1, K_2\}$ and $\{F_3, L_1, L_2\}$ is restricted to the following two possibilities: (i) three matrices within one triple are identical (up to column permutations); (ii) two matrices are identical in each triple and all four MU bases $\{I_3, F_3, H_y, H_w\}$ are used.

If all matrices in one triple are the same, i.e. $K_1 = K_2 = I_3$, then H_9 is equivalent to the transposed Fourier family $(F_9^{(4)})^T$ of order 9, which depends on four real parameters.

Now suppose that $K_1 = I_3$ and $L_1 = F_3$. The only remaining choice for matrices K_2 and L_2, (if $K_2 \neq I_3$), that satisfy the MU conditions is $K_2 = H_y$ and $L_2 = H_w$ (or vice versa), with H_y and H_w defined in Eq. (3.17). Denoting the resulting matrix by S_9, we find

$$S_9 = \frac{1}{\sqrt{3}} \begin{pmatrix} F_3 & F_3 & H_w \\ F_3 & \omega F_3 & \omega^2 H_w \\ H_y^\dagger F_3 & \omega^2 H_y^\dagger F_3 & \omega H_y^\dagger H_w \end{pmatrix}. \tag{6.14}$$

After dephasing, the matrix S_9 takes the form

$$S_9 = \frac{1}{3}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & 1 & \omega & \omega^2 & \omega^2 & 1 & \omega \\ 1 & \omega^2 & \omega & 1 & \omega^2 & \omega & \omega^2 & \omega & 1 \\ 1 & 1 & 1 & \omega & \omega & \omega & \omega^2 & \omega^2 & \omega^2 \\ 1 & \omega & \omega^2 & \omega & \omega^2 & 1 & \omega & \omega^2 & 1 \\ 1 & \omega^2 & \omega & \omega & 1 & \omega^2 & \omega & 1 & \omega^2 \\ 1 & \omega & \omega & \omega^2 & 1 & 1 & -\omega & -1 & -1 \\ 1 & \omega^2 & 1 & \omega^2 & \omega & \omega^2 & -\omega^2 & -1 & -\omega^2 \\ 1 & 1 & \omega^2 & \omega^2 & \omega^2 & \omega & -\omega^2 & -\omega^2 & -1 \end{pmatrix}, \tag{6.15}$$

where $\omega = e^{2\pi i/3}$ is a *third* root of unity. Due to the negative signs in the bottom right block, S_9 is a Butson-Hadamard matrix containing *sixth* roots of unity, i.e. $S_9 \in BH(9,6)$. We find the defect of this matrix to be $d(S_9) = 0$ implying that S_9 is *isolated.*

Proposition 6.3.1. *The matrix S_9 is inequivalent to $F_9^{(4)}$, B_9 and N_9.*

Since $F_9^{(6)}$ and B_9 have non-zero defects and N_9 contains only tenth roots of unity, it is clear that S_9 is inequivalent to any known complex Hadamard matrix in dimension $d = 9$. The only other isolated complex Hadamard matrix known for $d = 9$, i.e. N_9, was found by a numerical search in [9]. As far as we are aware, the matrix S_9 has not been published previously.

6.3.4 Dimension ten

The known Hadamard matrices in dimension ten include the Fourier family $F_{10}^{(4)}$ and its transpose $(F_{10}^{(4)})^T$, the family $D_{10}^{(8)}$ found by Diţă [29] and a family $D_{10}^{(3)}$ stemming from D_{10} [84]. There is also an isolated matrix N_{10A}, a family $N_{10B}^{(3)}$ found originally in [9] and parameterised in [57], and $G_{10}^{(1)}$ [57]. Furthermore, there are the Butson-Hadamard matrices $X_{10} \in BH(10,5)$ [7] and $W' \in BH(10,6)$ [27]. Within the continuous families, several Butson-type matrices exist: $D_{10} \in BH(10,4)$, $F_2 \otimes F_5 \simeq F_{10} \in BH(10,10)$, and those contained in $D_{10}^{(8)}$, e.g. $H_{10}^{(\omega)}$, $d_{10}^{(\omega)} \in BH(10,6)$ given in [29].

In the following, we construct a complex Hadamard matrix of Butson-type based on the block matrix

$$H_{10} = \frac{1}{\sqrt{2}} \begin{pmatrix} F_5 & L_1 \\ K_1^\dagger F_5 & -K_1^\dagger L_1 \end{pmatrix}, \tag{6.16}$$

where it is necessary that the pair of (5×5) matrices $\{I_5, K_1\}$ is MU to the pair of (5×5) matrices $\{F_5, L_1\}$. Here, I_5 is the identity matrix and F_5 the Fourier matrix,

$$F_5 \equiv \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega & \omega^3 \\ 1 & \omega^3 & \omega & \omega^4 & \omega^2 \\ 1 & \omega^4 & \omega^3 & \omega^2 & \omega \end{pmatrix}, \tag{6.17}$$

with $\omega = e^{2\pi i/5}$ a fifth root of unity. Assuming that K_1 and L_1 are not identical to I_5 and F_5, respectively, one choice is to require that the matrices within the set $\{I_5, F_5, K_1, L_1\}$ are pairwise MU.

In dimension five, the complete set of six MU bases can be written as

$$\{I_5, F_5, H_1, H_2, H_3, H_4\}, \tag{6.18}$$

where H_i are the complex Hadamard matrices of order five given by

$$H_1 = DF_5, \quad H_2 = D^2 F_5, \quad H_3 = D^3 F_5, \quad H_4 = D^4 F_5, \tag{6.19}$$

and with a diagonal matrix,

$$D = \mathrm{diag}(1, \omega, \omega^4, \omega^4, \omega). \tag{6.20}$$

This characterisation of the complete set of MU bases is based on a construction in [19]. By choosing $K_1 = H_3$ and $L_1 = H_4$, the matrix H_{10} becomes

$$S_{10} = \frac{1}{\sqrt{2}} \begin{pmatrix} F_5 & H_4 \\ H_3^\dagger F_5 & -H_3^\dagger H_4 \end{pmatrix}, \tag{6.21}$$

which has the dephased form

$$S_{10} = \frac{1}{\sqrt{10}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^4 & 1 & \omega & \omega^2 & \omega^3 \\ 1 & \omega^2 & \omega^4 & \omega & \omega^3 & \omega & \omega^3 & 1 & \omega^2 & \omega^4 \\ 1 & \omega^3 & \omega & \omega^4 & \omega^2 & \omega & \omega^4 & \omega^2 & 1 & \omega^3 \\ 1 & \omega^4 & \omega^3 & \omega^2 & \omega & \omega^4 & \omega^3 & \omega^2 & \omega & 1 \\ 1 & \omega^3 & \omega^2 & \omega^2 & \omega^3 & 1 & \omega & \omega^4 & \omega^4 & \omega \\ 1 & \omega^2 & 1 & \omega^4 & \omega^4 & \omega^3 & \omega^2 & \omega^3 & \omega & \omega \\ 1 & \omega & \omega^3 & \omega & 1 & \omega^2 & \omega^4 & \omega^3 & \omega^4 & \omega^2 \\ 1 & 1 & \omega & \omega^3 & \omega & \omega^2 & \omega^2 & \omega^4 & \omega^3 & \omega^4 \\ 1 & \omega^4 & \omega^4 & 1 & \omega^2 & \omega^3 & \omega & \omega & \omega^3 & \omega^2 \end{pmatrix}, \qquad (6.22)$$

where $\omega = e^{2\pi i/5}$ is a *fifth* root of unity.

Proposition 6.3.2. *The matrix S_{10} is inequivalent to $F_{10}^{(4)}$, $(F_{10}^{(4)})^T$, $D_{10}^{(3)}$, $D_{10}^{(8)}$, N_{10A}, $N_{10B}^{(3)}$, $G_{10}^{(1)}$ and W'.*

The matrix S_{10} is found to be *isolated* and contains only fifth roots of unity, therefore it is inequivalent to any of the complex Hadamard matrices listed in the proposition. However, we have not been able to show whether it is equivalent (or not) to the isolated Butson-type matrix $X_{10} \in BH(10, 5)$ or the matrix B_{10} given in Appendix D.

A different choice of the matrices K_1 and L_1, for example, $K_1 = H_1$ and $L_1 = H_2$, leads to the block matrix

$$S'_{10} = \frac{1}{\sqrt{2}} \begin{pmatrix} F_5 & H_2 \\ H_1^\dagger F_5 & -H_1^\dagger H_2 \end{pmatrix}, \qquad (6.23)$$

which in dephased form is given by

$$S'_{10} = \frac{1}{\sqrt{10}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^2 & \omega^3 & \omega^4 & 1 & \omega \\ 1 & \omega^2 & \omega^4 & \omega & \omega^3 & \omega^3 & 1 & \omega^2 & \omega^4 & \omega \\ 1 & \omega^3 & \omega & \omega^4 & \omega^2 & \omega^3 & \omega & \omega^4 & \omega^2 & 1 \\ 1 & \omega^4 & \omega^3 & \omega^2 & \omega & \omega^2 & \omega & 1 & \omega^4 & \omega^3 \\ 1 & \omega^4 & \omega & \omega & \omega^4 & -1 & -\omega & -\omega^4 & -\omega^4 & -\omega \\ 1 & \omega & 1 & \omega^2 & \omega^2 & -\omega^2 & -\omega & -\omega^2 & -1 & -1 \\ 1 & \omega^3 & \omega^4 & \omega^3 & 1 & -\omega^3 & -1 & -\omega^4 & -1 & -\omega^3 \\ 1 & 1 & \omega^3 & \omega^4 & \omega^3 & -\omega^3 & -\omega^3 & -1 & -\omega^4 & -1 \\ 1 & \omega^2 & \omega^2 & 1 & \omega & -\omega^2 & -1 & -1 & -\omega^2 & -\omega \end{pmatrix}, \tag{6.24}$$

with $\omega = e^{2\pi i/5}$ a fifth root of unity. This matrix is a member of the family $BH(10, 10)$ and, with a defect $d(S'_{10}) = 8$, the maximum dimension of any smooth manifold stemming from S'_{10} will be eight. Several other matrices of the form $BH(10, 10)$ exist but we are not able to determine whether S'_{10} is equivalent to any of them.

Any choice of K_1 and L_1 from the set of MU bases $\{F_5, H_1, H_2, H_3, H_4\}$ will result in a Butson-type matrix of the form $BH(10, 5)$ or $BH(10, 10)$. It would be interesting to see if the various combinations of K_1 and L_1 result in further new inequivalent complex Hadamard matrices.

6.3.5 Dimension fourteen

The known complex Hadamard matrices of order fourteen are the six-parameter Fourier family $F_{14}^{(6)}$ and its transpose $(F_{14}^{(6)})^T$, the family $D_{14}^{(6)}$ found in [84], and a set of at least eight isolated matrices $L_{14X}^{(0)}$ found in [57]. In addition, there are several Diţă-type matrices, listed in [21], obtained from Diţă's method of Corollary 6.1.2 using the Fourier matrix F_2 and any Hadamard matrix of order seven.

The matrix we construct from Theorem 6.2.1 consists of four blocks,

$$H_{14} = \frac{1}{\sqrt{2}} \begin{pmatrix} F_7 & L_1 \\ K_1^\dagger F_7 & -K_1^\dagger L_1 \end{pmatrix}, \tag{6.25}$$

where the Fourier matrix of order seven is given by

$$F_7 = \frac{1}{\sqrt{7}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 \\ 1 & \omega^2 & \omega^4 & \omega^6 & \omega & \omega^3 & \omega^5 \\ 1 & \omega^3 & \omega^6 & \omega^2 & \omega^5 & \omega & \omega^4 \\ 1 & \omega^4 & \omega & \omega^5 & \omega^2 & \omega^6 & \omega^3 \\ 1 & \omega^5 & \omega^3 & \omega & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega \end{pmatrix}, \tag{6.26}$$

with $\omega = e^{2\pi i/7}$, and the (7×7) matrices K_1 and L_1 are chosen from the complete set of eight MU bases of the space $\mathbb{C}^7$.

Let us denote the complete set of MU bases by $\{I_7, F_7, H_1, H_2, H_3, H_4, H_5, H_6\}$ where

$$H_j = D^j F_7 \tag{6.27}$$

and

$$D = \mathrm{diag}(1, 1, \omega, \omega^3, \omega^6, \omega^3, \omega), \tag{6.28}$$

with $j = 1, \ldots, 6$. The diagonal D is based on the construction of a complete sets of MU bases in prime dimensions presented in [6]. By choosing $K_1 = H_1$ and $L_1 = H_2$, we find a complex Hadamard matrix which, after dephasing, reads explicitly

$$S_{14} = \frac{1}{\sqrt{14}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 \\ 1 & \omega^2 & \omega^4 & \omega^6 & \omega & \omega^3 & \omega^5 & \omega^2 & \omega^4 & \omega^6 & \omega & \omega^3 & \omega^5 & 1 \\ 1 & \omega^3 & \omega^6 & \omega^2 & \omega^5 & \omega & \omega^4 & \omega^6 & \omega^2 & \omega^5 & \omega & \omega^4 & 1 & \omega^3 \\ 1 & \omega^4 & \omega & \omega^5 & \omega^2 & \omega^6 & \omega^3 & \omega^5 & \omega^2 & \omega^6 & \omega^3 & 1 & \omega^4 & \omega \\ 1 & \omega^5 & \omega^3 & \omega & \omega^6 & \omega^4 & \omega^2 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^5 & \omega^3 & \omega \\ 1 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega & \omega^2 & \omega & 1 & \omega^6 & \omega^5 & \omega^4 & \omega^3 \\ 1 & \omega & \omega^3 & \omega^6 & \omega^3 & \omega & 1 & \omega^5 & \omega^5 & \omega^4 & \omega^2 & \omega^6 & \omega^2 & \omega^4 \\ 1 & 1 & \omega & \omega^3 & \omega^6 & \omega^3 & \omega & \omega^4 & \omega^5 & \omega^5 & \omega^4 & \omega^2 & \omega^6 & \omega^2 \\ 1 & \omega^6 & \omega^6 & 1 & \omega^2 & \omega^5 & \omega^2 & \omega & \omega^3 & \omega^4 & \omega^4 & \omega^3 & \omega & \omega^5 \\ 1 & \omega^5 & \omega^4 & \omega^4 & \omega^5 & 1 & \omega^3 & \omega^3 & \omega^6 & \omega & \omega^2 & \omega^2 & \omega & \omega^6 \\ 1 & \omega^4 & \omega^2 & \omega & \omega & \omega^2 & \omega^4 & \omega^3 & 1 & \omega^3 & \omega^5 & \omega^6 & \omega^6 & \omega^5 \\ 1 & \omega^3 & 1 & \omega^5 & \omega^4 & \omega^4 & \omega^5 & \omega & \omega^6 & \omega^3 & \omega^6 & \omega & \omega^2 & \omega^2 \\ 1 & \omega^2 & \omega^5 & \omega^2 & 1 & \omega^6 & \omega^6 & \omega^4 & \omega^3 & \omega & \omega^5 & \omega & \omega^3 & \omega^4 \end{pmatrix}, \qquad (6.29)$$

with $\omega = e^{2\pi i/7}$. This is an *isolated* Butson-type complex Hadamard matrix of the form $BH(14, 7)$.

Proposition 6.3.3. *The matrix S_{14} is inequivalent to $F_{14}^{(6)}$, $(F_{14}^{(6)})^T$, $D_{14}^{(5)}$, $L_{14X}^{(0)}$ and every Diţă-type matrix given in [21].*

Since S_{14} and $L_{14X}^{(0)}$ contain different roots of unity they are inequivalent. All other known matrices listed in the proposition are contained in *families* of complex Hadamard matrices, thus, they are inequivalent to S_{14}. However, it is not known whether S_{14} is equivalent to the Butson-Hadamard matrix B_{14} given in Appendix D.

We can construct further complex Hadamard matrices by choosing different MU bases for K_1 and L_1, e.g. if $K_1 = H_1$ and $L_1 = H_4$, the resulting matrix in dephased form is

$$S'_{14} = \frac{1}{\sqrt{14}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 \\ 1 & \omega^2 & \omega^4 & \omega^6 & \omega & \omega^3 & \omega^5 & \omega^4 & \omega^6 & \omega & \omega^3 & \omega^5 & 1 & \omega^2 \\ 1 & \omega^3 & \omega^6 & \omega^2 & \omega^5 & \omega & \omega^4 & \omega^5 & \omega & \omega^4 & 1 & \omega^3 & \omega^6 & \omega^2 \\ 1 & \omega^4 & \omega & \omega^5 & \omega^2 & \omega^6 & \omega^3 & \omega^3 & 1 & \omega^4 & \omega & \omega^5 & \omega^2 & \omega^6 \\ 1 & \omega^5 & \omega^3 & \omega & \omega^6 & \omega^4 & \omega^2 & \omega^5 & \omega^3 & \omega & \omega^6 & \omega^4 & \omega^2 & 1 \\ 1 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega & \omega^4 & \omega^3 & \omega^2 & \omega & 1 & \omega^6 & \omega^5 \\ 1 & \omega & \omega^3 & \omega^6 & \omega^3 & \omega & 1 & -\omega^3 & -\omega & -\omega & -\omega^3 & -1 & -\omega^6 & -1 \\ 1 & 1 & \omega & \omega^3 & \omega^6 & \omega^3 & \omega & -1 & -\omega^3 & -\omega & -\omega & -\omega^3 & -1 & -\omega^6 \\ 1 & \omega^6 & \omega^6 & 1 & \omega^2 & \omega^5 & \omega^2 & -\omega^5 & -\omega^6 & -\omega^2 & -1 & -1 & -\omega^2 & -\omega^6 \\ 1 & \omega^5 & \omega^4 & \omega^4 & \omega^5 & 1 & \omega^3 & -\omega^4 & -\omega^3 & -\omega^4 & -1 & -\omega^5 & -\omega^5 & -1 \\ 1 & \omega^4 & \omega^2 & \omega & \omega & \omega^2 & \omega^4 & -\omega^4 & -\omega & -1 & -\omega & -\omega^4 & -\omega^2 & -\omega^2 \\ 1 & \omega^3 & 1 & \omega^5 & \omega^4 & \omega^4 & \omega^5 & -\omega^5 & -1 & -\omega^4 & -\omega^3 & -\omega^4 & -1 & -\omega^5 \\ 1 & \omega^2 & \omega^5 & \omega^2 & 1 & \omega^6 & \omega^6 & -1 & -1 & -\omega^2 & -\omega^6 & -\omega^5 & -\omega^6 & -\omega^2 \end{pmatrix}, \tag{6.30}$$

with $\omega = e^{2\pi i/7}$. This is a Butson-Hadamard matrix of the form $BH(14, 14)$, and has a defect of 12. It is unknown if S'_{14} is equivalent to a $BH(14, 14)$ matrix contained within an existing family of Hadamard matrices.

6.3.6 Dimension fifteen

The only known complex Hadamard matrices of order fifteen are the eight-parameter Fourier family $F_{15}^{(8)}$, stemming from the Fourier matrix $F_{15} \simeq F_3 \otimes F_5 \in BH(15, 15)$, and the transposed Fourier family $(F_{15}^{(8)})^T$. To construct a new (15×15) complex Hadamard matrix by means of Theorem 6.2.1, we use the block matrix

$$H_{15} = \frac{1}{\sqrt{3}} \begin{pmatrix} F_5 & L_1 & L_2 \\ K_1^\dagger F_5 & \alpha K_1^\dagger L_1 & \alpha^2 K_1^\dagger L_2 \\ K_2^\dagger F_5 & \alpha^2 K_2^\dagger L_1 & \alpha K_2^\dagger L_2 \end{pmatrix}, \tag{6.31}$$

where $\alpha = e^{2\pi i/3}$ is a third root of unity, I_5, F_5, K_1, K_2, L_1 and L_2 are (5×5) matrices including the identity matrix I_5 and the Fourier matrix F_5 defined in Eq. (6.17). The set $\{I_5, K_1, K_2\}$ is MU to the set $\{F_5, L_1, L_2\}$.

If we use the *complete* set of six MU bases of the space $\mathbb{C}^5$, $\{I_5, F_5, H_1, H_2, H_3, H_4\}$, corresponding to $K_1 = H_1$, $K_2 = H_2$, $L_1 = H_3$ and $L_2 = H_4$, as defined in Eq. (6.19), the resulting complex Hadamard matrix becomes

$$S_{15} = \frac{1}{\sqrt{3}} \begin{pmatrix} F_5 & H_3 & H_4 \\ H_1^\dagger F_5 & \alpha H_1^\dagger H_3 & \alpha^2 H_1^\dagger H_4 \\ H_2^\dagger F_5 & \alpha^2 H_2^\dagger H_3 & \alpha H_2^\dagger H_4 \end{pmatrix}. \tag{6.32}$$

Apart from a factor $1/\sqrt{15}$, its dephased form reads explicitly

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & \omega^3 & \omega^6 & \omega^9 & \omega^{12} & \omega^9 & \omega^{12} & 1 & \omega^3 & \omega^6 & \omega^{12} & 1 & \omega^3 & \omega^6 & \omega^9 \\
1 & \omega^6 & \omega^{12} & \omega^3 & \omega^9 & \omega^6 & \omega^{12} & \omega^3 & \omega^9 & 1 & \omega^3 & \omega^9 & 1 & \omega^6 & \omega^{12} \\
1 & \omega^9 & \omega^3 & \omega^{12} & \omega^6 & \omega^6 & 1 & \omega^9 & \omega^3 & \omega^{12} & \omega^3 & \omega^{12} & \omega^6 & 1 & \omega^9 \\
1 & \omega^{12} & \omega^9 & \omega^6 & \omega^3 & \omega^9 & \omega^6 & \omega^3 & 1 & \omega^{12} & \omega^{12} & \omega^9 & \omega^6 & \omega^3 & 1 \\
1 & \omega^{12} & \omega^3 & \omega^3 & \omega^{12} & -\omega^5 & -\omega^{14} & -\omega^{11} & -\omega^{14} & -\omega & -\omega^{10} & -\omega & -\omega^4 & -\omega^4 & -\omega \\
1 & \omega^3 & 1 & \omega^6 & \omega^6 & -\omega^2 & -\omega^8 & -\omega^2 & -\omega^{14} & -\omega^{14} & -\omega^4 & -\omega^{13} & -\omega^4 & -\omega^7 & -\omega^7 \\
1 & \omega^9 & \omega^{12} & \omega^9 & 1 & -\omega^8 & -\omega^{11} & -\omega^2 & -\omega^{11} & -\omega^8 & -\omega & -\omega^{13} & -\omega^7 & -\omega^{13} & -\omega \\
1 & 1 & \omega^9 & \omega^{12} & \omega^9 & -\omega^8 & -\omega^8 & -\omega^{11} & -\omega^2 & -\omega^{11} & -\omega & -\omega & -\omega^{13} & -\omega^7 & -\omega^{13} \\
1 & \omega^6 & \omega^6 & 1 & \omega^3 & -\omega^2 & -\omega^{14} & -\omega^{14} & -\omega^2 & -\omega^8 & -\omega^4 & -\omega^7 & -\omega^7 & -\omega^4 & -\omega^{13} \\
1 & \omega^6 & \omega^9 & \omega^9 & \omega^6 & -\omega^{10} & -\omega^{13} & -\omega^7 & -\omega^7 & -\omega^{13} & \omega^5 & \omega^{14} & \omega^{11} & \omega^{11} & \omega^{14} \\
1 & \omega^9 & 1 & \omega^3 & \omega^3 & -\omega^7 & -\omega^4 & -\omega^7 & -\omega & -\omega & \omega^8 & \omega^{14} & \omega^8 & \omega^5 & \omega^5 \\
1 & \omega^{12} & \omega^6 & \omega^{12} & 1 & -\omega^{13} & -\omega^4 & -\omega & -\omega^4 & -\omega^{13} & \omega^2 & \omega^5 & \omega^{11} & \omega^5 & \omega^2 \\
1 & 1 & \omega^{12} & \omega^6 & \omega^1 2 & -\omega^{13} & -\omega^{13} & -\omega^4 & -\omega & -\omega^4 & \omega^2 & \omega^2 & \omega^5 & \omega^{11} & \omega^5 \\
1 & \omega^3 & \omega^3 & 1 & \omega^9 & -\omega^7 & -\omega & -\omega & -\omega^7 & -\omega^4 & \omega^8 & \omega^5 & \omega^5 & \omega^8 & \omega^{14}
\end{pmatrix}, \tag{6.33}$$

where $\omega = e^{2\pi i/15}$ is now a *fifteenth* root of unity. Since all matrix elements can be written in terms of 30th roots of unity, S_{15} is an example of a Butson-Hadamard matrix $BH(15, 30)$. The vanishing defect of this matrix, i.e. $d(S_{15}) = 0$, implies that S_{15} is *isolated.* This property excludes S_{15} from being a member of either of the affine families $F_{15}^{(8)}$ or $(F_{15}^{(8)})^T$.

Proposition 6.3.4. *The matrix S_{15} is inequivalent to $F_{15}^{(8)}$ and $(F_{15}^{(8)})^T$.*

One could produce additional complex Hadamard matrices by choosing different combinations of MU bases from the complete set of six, such as $K_1 = I_5$ or $L_1 = F_3$. It is likely that various inequivalent matrices will result from these choices.

6.4 Examples: dimensions $d > 15$, and further generalisations

The construction of the matrices S_6, S_9 and S_{15} has a common feature: in each case, the matrices $K_0, \ldots, K_{p-1}, L_0, \ldots, L_{p-1}$ used to construct the blocks of the Hadamard matrix in Theorem 6.2.1 include a *complete* set of $(q+1)$ MU bases of the space $\mathbb{C}^q$. For the cases $d = 6$ and $d = 15$, i.e. $q = 2p - 1$, complete sets of MU bases in dimension three and five are used, respectively, resulting in the isolated matrices S_6 and S_{15}. Furthermore, in the case $d = 9$, where $q < 2p - 1$, a complete set of four MU bases in dimension three is used, and again we find an isolated Hadamard matrix, namely S_9.

Thus, one might expect additional isolated complex Hadamard matrices to emerge for larger composite dimensions whenever its factors are related by $q \leq 2p - 1$. We have been able to confirm this property for all primes p, q, with $pq < 100$ and $q \leq 2p - 1$, excluding the case $d = 4$. The first three examples are covered by S_6, S_9 and S_{15} which we already know are isolated. The remaining five matrices S_{25}, S_{35}, S_{49}, S_{77} and S_{91}, also turn out to be *isolated*. We construct these matrices as follows:

- S_{25} is derived from the complete set of six MU bases I_5, F_5 and $H_j = D^j F_5$, $j = 1 \ldots 4$, where $D = \text{diag}(1, \omega, \omega^4, \omega^4, \omega)$ and $\omega = e^{2\pi i/5}$. The matrices K_n, for $n = 0 \ldots 4$, are chosen as I_5, I_5, I_5, H_1, H_2, respectively, and L_n as F_5, F_5, F_5, H_3, H_4, respectively.

- S_{35} uses the complete set of eight MU bases I_7, F_7 and $H_j = D^j F_7$, $j = 1 \ldots 6$, where $D = \text{diag}(1, 1, \omega, \omega^3, \omega^6, \omega^3, \omega)$ and $\omega = e^{2\pi i/7}$. The matrices K_n, for $n = 0 \ldots 4$, are chosen as I_7, I_7, H_1, H_2, H_3, and L_n as F_7, F_7, H_4, H_5, H_6, respectively.

- S_{49} is constructed from the same complete set of MU bases used for S_{35}, and we choose K_n as $I_7, I_7, I_7, I_7, H_1, H_2, H_3$, and L_n as $F_7, F_7, F_7, F_7, H_3, H_4, H_5$, with $n = 0 \ldots 6$, respectively.

- S_{77} uses a complete set of twelve MU bases given by I_{11}, F_{11} and H_j, $j = 1 \ldots 10$ with $D = \text{diag}(1, 1, \omega, \omega^3, \omega^6, \omega^{10}, \omega^4, \omega^{10}, \omega^6, \omega^3, \omega)$ and $\omega = e^{2\pi i/11}$. The matrices K_n, for $n = 0 \ldots 6$, are chosen as $I_{11}, I_{11}, H_1, H_2, H_3, H_4, H_5$ and L_n as $F_{11}, F_{11}, H_6, H_7, H_8, H_9$, H_{10}, respectively.

- S_{91} is based on the complete set of fourteen MU bases in $\mathbb{C}^{13}$, i.e. the identity I_{13}, the Fourier matrix F_{13}, and the matrices $H_j = D^j F_{13}$ for $j = 1 \ldots 12$, where the diagonal matrix is given by $D = \text{diag}(1, 1, \omega, \omega^3, \omega^6, \omega^{10}, \omega^2, \omega^8, \omega^2, \omega^{10}, \omega^6, \omega^3, \omega)$ and $\omega = e^{2\pi i/13}$. The matrices $K_1, \ldots, K_6, L_1, \ldots, L_6$, correspond to $H_1, \ldots, H_{12}$, respectively.

All these isolated matrices are of Butson-Hadamard type with $S_{25} \in BH(25, 10)$, $S_{35} \in BH(35, 70)$, $S_{49} \in BH(49, 14)$, $S_{77} \in BH(77, 154)$ and $S_{91} \in BH(91, 182)$. They may have smaller roots of unity if their matrix elements contain no entries equal to (-1). The matrix S_{91} is similar to S_6 and S_{15} in the sense that the prime factors of $d = 91$ satisfy the equality $q = 2p - 1$, meaning that each MU basis from the complete set is used exactly once. For the other isolated matrices, the factors satisfy the inequality $q < 2p - 1$, which implies that some MU bases are used more than once in the set $K_0, \ldots, L_{p-1}$. In this case, there are additional choices for the bases used; different combinations may lead to further inequivalent isolated complex Hadamard matrices.

So far, we have applied Theorem 6.2.1 mainly to product dimensions $4 \leq d \leq 15$ or when $d = pq < 100$ and $q \leq 2p - 1$. To explore whether the latter constraint on the factors p and q is necessary, we have constructed Hadamard matrices in all other composite dimension $d < 100$ for $p, q \leq 13$. In each of these cases, i.e. $d = 21$, 22, 26, 33, 39, 55 and 65, we were able to identify isolated Hadamard matrices. In addition, it is also possible to construct Hadamard matrices with non-zero defects, simply by selecting different sets of MU bases for $K_0, \ldots, L_{p-1}$. Thus, the theorem is potentially the source of infinitely many new Hadamard matrices in *arbitrary* product dimensions.

Interestingly, the method is not limited to dimensions of the form $d = pq$: if the numbers p and q are composite, it is likely that additional, possibly inequivalent complex Hadamard matrices can be constructed which relate to different factorisations of the dimension, such as $2 \times 6 = 3 \times 4$ when $d = 12$. Furthermore, it has been shown in [46] that *inequivalent* complete sets of MU bases exist for large prime-power dimensions, possibly leading to yet more inequivalent Hadamard matrices. One could also try to create continuous families of complex Hadamard matrices if sets of four or more MU bases exist which contain free parameters after dephasing.

Finally, another generalisation of Theorem 6.2.1 can be achieved as follows. The Hadamard matrices we have constructed are derived from product bases which tensor each vector in an orthonormal basis of $\mathbb{C}^p$ with an orthonormal basis of $\mathbb{C}^q$ (cf. Eqs. (6.5,6.6)). However, other types of product bases exist; for example, one could take vectors from *different* orthonormal bases in $\mathbb{C}^p$ and tensor them with vectors from *one* basis in $\mathbb{C}^q$. The classification of all product bases in the space $\mathbb{C}^2 \otimes \mathbb{C}^3$, up to local equivalence transformations, contains a number of examples of these so-called *indirect* product bases (cf. Lemma 3.2.2). Thus, alternative block structures may be allowed in Theorem 6.2.1, potentially leading to other Hadamard matrices.

6.5 Summary

The main results of this chapter are (i) a new general construction of complex Hadamard matrices in composite dimensions $d = pq$ (p, q prime) described in Theorem 6.2.1, and (ii) the explicit derivation of various new complex Hadamard matrices as a consequence of this theorem. The construction relies on the simple idea that a suitable unitary transformation maps a pair of MU *product* bases to its standard form in which the vectors of one basis turn into the columns of a complex Hadamard matrix. It becomes possible to *systematically* construct new Hadamard matrices many of which are isolated. Previous examples of isolated Hadamard matrices have been found by trial and error [89] or from numerical methods [9].

To illustrate the approach we first derive some known results in low dimensions. In particular, we find the complete family of complex Hadamard matrices when $d = 4$, and in dimension six we find the isolated matrix S_6. We then proceed to higher dimensions, obtaining isolated Hadamard matrices of order 9, 10, 14 and 15. Two of these are new isolated Butson-type Hadamard matrices, namely $S_9 \in BH(9,6)$ and $S_{15} \in BH(15,30)$, while $S_{10} \in BH(10,5)$ and $S_{14} \in B(14,7)$ are shown to be inequivalent to nearly all known Hadamard matrices of their order. However, we cannot exclude the equivalence of S_{10} to B_{10} or X_{10}, and of S_{14} to B_{14}.

In dimensions $d = 10$ and $d = 14$, there is some flexibility in selecting suitable subsets of MU bases when applying Theorem 6.2.1. This enables us to construct two non-isolated Hadamard matrices S'_{10} and S'_{14}, with defects equal to 8 and 12, respectively. Further research is needed to understand which choices of MU bases will lead to inequivalent Hadamard matrices.

Whenever the factors in the product dimension $d = pq$ are related by $q \leq 2p - 1$, the set $K_0, \ldots, K_{p-1}, L_0, \ldots, L_{p-1}$ given in Theorem 6.2.1 can accommodate a *complete* set of MU bases for the space $\mathbb{C}^q$. We speculate that in these cases, with the exception of dimension four, Theorem 6.2.1 will always give rise to an isolated Hadamard matrix. This expectation has been confirmed for all matrices of order $d = pq < 100$ that satisfy $q \leq 2p-1$. In these cases, the matrices S_6, S_9, and S_{15}, as well as S_{25}, S_{35}, S_{49}, S_{77} and S_{91} all turn out to be isolated, and they include the largest known examples of isolated Hadamard matrices (as far as we know). What is more, we are also able to generate isolated (and non-isolated) Hadamard matrices for dimensions $d = 21$, 22, 26, 33, 39, 55 and 65, giving rise to a total of 16 isolated complex Hadamard matrices. Twelve of these are new, while the remaining four, namely $S_{10}, S_{14}, S_{22}, S_{26} \in BH(2p, p)$, may be equivalent to matrices resulting from Butson's construction.

Throughout this chapter we have limited our search to Butson-type Hadamard matrices. However, the method given in Theorem 6.2.1 covers a much wider class of complex Hadamard matrices. We expect that many other examples of more general Hadamard matrices can be found by extending the choice for the unitary matrices K_n and L_n.

Chapter 7

Summary and outlook

In this thesis we have focused on the existence problem of complete sets of MU bases in dimension six. While it remains unknown if one can construct more than three MU bases in this case, we have made some progress which rules out the existence of a certain class of bases. In particular, we have restricted our studies to separable states and proved several non-existence results for complete sets containing MU product bases.

The landscape of the existence problem for composite dimensions is described in some detail in Chapter 2. Most of the progress in recent years relies on imposing certain assumptions on the construction of MU bases. For example, one can construct a complete set in prime and prime-power dimensions by partitioning a *nice error basis* into commuting sets of matrices. However, a nice error basis in dimension six does not yield a complete set (Theorem 2.4.2). Similarly, by partitioning sets of *monomial* matrices of order six into classes of commuting matrices, one can construct no more than three MU bases (Theorem 2.1.2). These are two of the very few analytic non-existence results for composite dimensions.

Most other non-existence results in dimension six rely on various computer-aided calculations and show that certain pairs of MU bases do not extend to a complete set. This is most notably demonstrated in a proof by Matolsci *et al.* showing that the set of all pairs containing the identity matrix and a member of the two-parameter Fourier family does not extend to a quadruple of MU bases (Theorem 2.5.1).

The results in this thesis use similar methods to those described, in the sense that certain assumptions are made during the construction; in our case this assumption is the separability of the states. This is particularly interesting in light of a recent result requiring that a complete set of MU bases must contain a fixed amount of entanglement. In addition, we prove that certain pairs and triples of MU bases do not extend to a complete set. All our results are rigorous, however some are entirely analytic and others rely on computer-aided calculations.

We now give a brief summary of the main results in this thesis. For a more detailed discussion see the summary section provided at the end of each chapter. In Chapter 3 our main results include a complete classification of all pairs and triples of MU product bases in dimensions six: there exist four families of pairs (Theorem 3.5.1) and two inequivalent triples (Theorem 3.5.2). Subsequently, we conclude that no MU product triple can be extended by a single MU vector, i.e. Theorem 3.6.1. This proof relies on a computer-aided result provided by Grassl.

In the following chapter we prove that if a complete set of seven MU bases exists in dimension six, it contains at most one product basis (Theorem 4.0.1). Again, this result relies on computer-aided (rigorous) results: firstly, a proof by Matolsci *et al.* described above, and secondly, a proof by Brierley *et al.* that the isolated matrix S_6 together with the identity do not extend beyond a MU triple. This theorem is our strongest non-existence result.

In Chapter 5 we conclude our studies on product bases by providing an *analytic* proof that no MU product triple can be extended by a single MU vector, originally proved in Chapter 3 using a computer-algebraic approach. In addition, we strengthen this statement by showing that a product constellation $\{5,5,4\}_6^{\otimes}$ containing two bases and a set of four orthonormal states cannot be part of a complete set of seven MU bases, i.e. Theorem 5.2.1.

In the penultimate chapter, our focus shifts from MU bases to complex Hadamard matrices, and from dimension six to general composite dimensions of the form $d = pq$, where p and q are prime. The main result, summarised by Theorem 6.2.1, is a new construction method for complex Hadamard matrices. What is surprising is that the construction yields at least one *isolated* Hadamard matrix for every tested dimension in the range $6 \leq d \leq 100$. These particular matrices are unusual since they are disconnected from any continuous family of Hadamard matrices, and very few have been found before.

There are several questions that arise naturally from our work on product bases. One avenue of future research could attempt to generalise our results for dimension six to arbitrary composite dimensions $d = pq$. In particular, a classification of all MU product bases for higher dimensions may be of interest. For this, we would need to extend several of our results, namely Lemma 3.2.2 and Theorem 3.3.2. The main difficulty is to prove the conjecture, stated in Chapter 3 (a generalisation of Theorem 3.3.2), that the product state $|\psi, \Psi\rangle \in \mathbb{C}^d$ is MU to the product basis $\{|\psi_i, \Psi_i\rangle\}$ if and only if $|\phi\rangle$ is MU to $|\psi_i\rangle \in \mathbb{C}^p$ and $|\Psi\rangle$ is MU to $|\Psi_i\rangle \in \mathbb{C}^q$, for any p and q prime. Unfortunately, our proof of Theorem 3.3.2 does not extend, at least in any obvious way, to higher dimensions. However, one might expect product bases in composite dimensions to possess a certain structure which, once understood, would simplify the problem and allow for a more elegant proof.

A generalisation of our non-existence results, e.g. Theorem 4.0.1, to higher dimensions is difficult, mainly due to the increase in computational complexity of the calculations. It is likely that analytic arguments will be necessary, and in some cases an entirely new approach. For example, in the six-dimensional case we show analytically that the product constellation $\{5, 4, 4\}_6^{\otimes}$ cannot extend to a complete set. Any stronger statements regarding product constellations seems surprisingly difficult and probably require an alternative approach.

Our work on complex Hadamard matrices (see Chapter 6) generalises the construction of certain pairs of MU product bases in dimension six to composite dimensions $d = pq$. As a result, we use Theorem 6.2.1 to construct new Butson-type matrices, where the elements of each matrix consist of r-th roots of unity. The restriction on the elements is self-imposed due to simplicity; by dropping this constraint and allowing the block matrices to consist of products of parameter-dependent Hadamard matrices, the construction method may lead to the discovery of new *families* of Hadamard matrices. In addition, one can easily generalise the construction method to matrices of order $d = p_1^{n_1} p_2^{n_2} \dots p_r^{n_r}$, where d is non-prime. Furthermore, in arbitrary composite dimensions there exist a wider variety of *indirect* product bases (see Lemma 3.2.2 for the six-dimensional examples). By choosing various pairs of these indirect product bases it is likely that one can build a whole new collection of Hadamard matrices.

While this thesis provides a classification of a particular type of MU bases in dimension six, namely product bases, a complete classification of all MU bases in dimension six remains an ambitious challenge. Needless to say, a solution to the existence problem for arbitrary composite dimensions seems quite far away. Nevertheless, the problem remains intriguing for a variety of reasons. We hope that the contributions made here prove useful for future work in this field.

Appendix A

Classification of all product bases

In this Appendix we derive all product bases in dimension six reported in Lemma 3.2.2. The six states $|\psi_j\rangle, j = 1\ldots6$, of a product basis $\{|\psi_j, \Psi_j\rangle\}$, defined in (3.30) must contain at least *two* (possibly identical) pairs of orthogonal states. If there was only one pair (with the remaining four states of the space $\mathbb{C}^2$ non-orthogonal), the orthogonality conditions (3.31) would require *four* orthogonal states $|\Psi_j\rangle \in \mathbb{C}^3$, which do not exist. Thus, denoting the orthogonal pairs by $\{|a\rangle, |a^\perp\rangle\}$ and $\{|b\rangle, |b^\perp\rangle\}$, the product basis must take the form

$$\Big\{|a, \Psi_1\rangle,\, |a^\perp, \Psi_2\rangle,\, |b, \Psi_3\rangle,\, |b^\perp, \Psi_4\rangle,\, |\psi_5, \Psi_5\rangle,\, |\psi_6, \Psi_6\rangle\Big\}. \tag{A.1}$$

The states $|\psi_5\rangle$ and $|\psi_6\rangle$ must also be an orthogonal pair. To see this, assume that they are skew (or identical) *and* they are both skew to the states $|a\rangle$ and $|b\rangle$; then the state $|\Psi_6\rangle$, for example, must be orthogonal to the orthonormal triple $\{|\Psi_1\rangle, |\Psi_3\rangle, |\Psi_5\rangle\}$, which is impossible. Here we have assumed that $|a\rangle$ and $|b\rangle$ are *not* orthogonal; if they are, we use the orthonormal triple $\{|\Psi_1\rangle, |\Psi_4\rangle, |\Psi_5\rangle\}$ instead. The same conclusion can be drawn if the states $|\psi_5\rangle$ and $|\psi_6\rangle$ are skew (or identical) but one of them coincides with any of the four states $|a\rangle$, $|b\rangle$, $|a^\perp\rangle$ or $|b^\perp\rangle$. Thus, we conclude that any product basis of the space $\mathbb{C}^6$ must be of the form

$$\Big\{|a, \Psi_1\rangle,\, |a^\perp, \Psi_2\rangle,\, |b, \Psi_3\rangle,\, |b^\perp, \Psi_4\rangle,\, |c, \Psi_5\rangle,\, |c^\perp, \Psi_6\rangle\Big\}. \tag{A.2}$$

Now it is obvious that we need to consider three different possibilities depending on how many of the three bases of the space $\mathbb{C}^2$ coincide.

Case 1: If all three bases coincide, we have

$$\Big\{ |a, \Psi_1\rangle,\ |a^\perp, \Psi_2\rangle,\ |a, \Psi_3\rangle,\ |a^\perp, \Psi_4\rangle,\ |a, \Psi_5\rangle,\ |a^\perp, \Psi_6\rangle \Big\} . \tag{A.3}$$

These six states are orthogonal only if the three states $|\Psi_1\rangle, |\Psi_3\rangle$ and $|\Psi_5\rangle$ are orthogonal to each other, as well as the triple $\{|\Psi_2\rangle, |\Psi_4\rangle, |\Psi_6\rangle\}$. Upon denoting the first triple by $\{|A\rangle, |A^\perp\rangle, |A^{\perp\!\!\perp}\rangle\}$, where $|A^{\perp\!\!\perp}\rangle \in \mathbb{C}^3$ is a vector orthogonal to $|A\rangle$ and $|A^\perp\rangle$, we obtain

$$\mathcal{B}_1 = \Big\{ |a, A\rangle,\ |a, A^\perp\rangle,\ |a, A^{\perp\!\!\perp}\rangle,\ |a^\perp, B\rangle,\ |a^\perp, B^\perp\rangle,\ |a^\perp, B^{\perp\!\!\perp}\rangle \Big\} , \tag{A.4}$$

also introducing an arbitrary second triple of orthogonal states. If the two triples coincide, we find the important special case of a direct product basis

$$\mathcal{B}_0 = \Big\{ |a, A\rangle,\ |a, A^\perp\rangle,\ |a, A^{\perp\!\!\perp}\rangle,\ |a^\perp, A\rangle,\ |a^\perp, A^\perp\rangle,\ |a^\perp, A^{\perp\!\!\perp}\rangle \Big\} , \tag{A.5}$$

Case 2: If only two of the bases in $\mathbb{C}^2$ coincide, we find

$$\Big\{ |a, \Psi_1\rangle,\ |a^\perp, \Psi_2\rangle,\ |b, \Psi_3\rangle,\ |b^\perp, \Psi_4\rangle,\ |b, \Psi_5\rangle,\ |b^\perp, \Psi_6\rangle \Big\} . \tag{A.6}$$

As in Case 1, each of the triples $\{|\Psi_1\rangle, |\Psi_3\rangle, |\Psi_5\rangle\}$ and $\{|\Psi_2\rangle, |\Psi_4\rangle, |\Psi_6\rangle\}$ must be an orthonormal basis of $\mathbb{C}^3$. However, we also need to have

$$\langle \Psi_1 | \Psi_4 \rangle = \langle \Psi_1 | \Psi_6 \rangle = 0 , \tag{A.7}$$

which means that $|\Psi_3\rangle$ and $|\Psi_5\rangle$ span the same subspace as $|\Psi_4\rangle$ and $|\Psi_6\rangle$. It follows that $|\Psi_1\rangle \equiv |\Psi_2\rangle$; upon calling this state $|A\rangle$, we are led to a new class of product bases of $\mathbb{C}^6$ given by

$$\mathcal{B}_2 = \Big\{ |a, A\rangle,\ |a^\perp, A\rangle,\ |b, A^\perp\rangle,\ |b^\perp, \hat{V} A^\perp\rangle,\ |b, A^{\perp\!\!\perp}\rangle,\ |b^\perp, \hat{V} A^{\perp\!\!\perp}\rangle \Big\} , \tag{A.8}$$

where $\hat{V}|A^\perp\rangle = \alpha|A^\perp\rangle + \beta|A^{\perp\!\!\perp}\rangle$ and $\hat{V}|A^{\perp\!\!\perp}\rangle = \bar{\beta}|A^\perp\rangle - \bar{\alpha}|A^{\perp\!\!\perp}\rangle$, i.e. $\hat{V}$ is any unitary transformation of the two-dimensional subspace of $\mathbb{C}^3$ orthogonal to the state $|A\rangle$.

Case 3: Finally, we consider the case where the three bases of the space $\mathbb{C}^2$ present in (A.2) are all different, meaning that $|a\rangle$, $|b\rangle$, and $|c\rangle$ are pairwise skew. Then, the orthogonality conditions directly imply that the triples $\{|\Psi_1\rangle, |\Psi_3\rangle, |\Psi_5\rangle\}$ and $\{|\Psi_2\rangle, |\Psi_4\rangle, |\Psi_6\rangle\}$ of orthogonal states must coincide. This leaves us with bases of the form

$$\mathcal{B}_3 = \Big\{ |a, A\rangle,\ |a^\perp, A\rangle,\ |b, A^\perp\rangle,\ |b^\perp, A^\perp\rangle,\ |c, A^{\perp\!\!\perp}\rangle,\ |c^\perp, A^{\perp\!\!\perp}\rangle \Big\}\,. \tag{A.9}$$

These three cases complete the construction of all product bases in dimension six. Using local equivalence transformations in analogy to the procedure used in Sec. 3.2.1, one can write the four sets of product bases as displayed in Lemma 3.2.2.

Appendix B

Derivation of all MU product pairs

In this Appendix we derive all pairs of MU product bases in dimension six by pairwise combining the orthonormal product bases $\mathcal{B}_0$ to $\mathcal{B}_3$, defined in Eqs. (A.5,A.4,A.8,A.9). In principle, we need to look at only 10 of the 16 pairs $\{\mathcal{B}_i;\mathcal{B}_j\}$, $i,j = 0\ldots 3$, since the order of the bases does not matter: the pairs $\{\mathcal{B}_i;\mathcal{B}_j\}$ and $\{\mathcal{B}_j;\mathcal{B}_i\}$ are equivalent for $i \neq j$. Using local equivalence transformations, each pair can be brought to the form $\{\mathcal{I}_i;\mathcal{B}_j\}$, $i \leq j$, where the bases $\mathcal{I}_0$ to $\mathcal{I}_3$ are those listed in Lemma 3.2.2. As shown in the main text, it is not actually necessary to consider the bases $\mathcal{I}_2$ and $\mathcal{B}_2$ at all, reducing the number of cases to six. Parameter ranges are assumed so that no pair occurs more than once.

• $\{\mathcal{I}_0;\mathcal{B}_0\}$: First we extend $\mathcal{I}_0$ to a pair of MU bases by combining it with

$$\mathcal{B}_0 = \Big\{|a,A\rangle,\, |a,A^\perp\rangle,\, |a,A^{\perp\!\!\perp}\rangle,\, |a^\perp,A\rangle,\, |a^\perp,A^\perp\rangle,\, |a^\perp,A^{\perp\!\!\perp}\rangle\Big\}\,. \tag{B.1}$$

The states of $\mathcal{B}_0$ are MU to those of the basis $\mathcal{I}_0$ if the pair of states $\{|a\rangle, |a^\perp\rangle\}$ is any basis of $\mathbb{C}^2$ associated with opposite points on the Bloch sphere, i.e. $|a\rangle = (|0_z\rangle + e^{i\mu}|1_z\rangle)/\sqrt{2}$ etc., and if the orthonormal basis $\{|A\rangle, |A^\perp\rangle, |A^{\perp\!\!\perp}\rangle\}$ is defined as in Eqs. (3.15) of Sec. 3.1.2.

A local transformation allows us to rotate the states $\{|a\rangle, |a^{\perp}\rangle\}$ into $\{|j_x\rangle\}$ and to simultaneously change the basis $\{|A\rangle, |A^{\perp}\rangle, |A^{\perp\!\!\perp}\rangle\}$ into the basis $\{|J_x\rangle\}$ of $\mathbb{C}^3$ so that we end up with the known Heisenberg-Weyl MU pair of direct product bases,

$$\mathcal{P}_0 \equiv \{|j_z, J_z\rangle;\ |j_x, J_x\rangle\}\,. \tag{B.2}$$

• $\{\mathcal{I}_0; \mathcal{B}_1\}$ and $\{\mathcal{I}_0; \mathcal{B}_3\}$: These cases will be covered by the pairs $\{\mathcal{I}_1; \mathcal{B}_1\}$ and $\{\mathcal{I}_1; \mathcal{B}_3\}$, respectively, since we can treat the basis $\mathcal{I}_0$ as a subset of $\mathcal{I}_1$.

We now construct the three pairs of indirect product bases that contain $\mathcal{I}_1 = \{|0_z, J_z\rangle, |1_z, \hat{U}J_z\rangle\}$ as the first basis, where the unitary $\hat{U}$ maps the basis $\{|J_z\rangle\}$ of the space $\mathbb{C}^3$ to another basis.

• $\{\mathcal{I}_1; \mathcal{B}_1\}$: In a first step, we act with a local unitary on the second basis

$$\mathcal{B}_1 = \Big\{|a, A\rangle,\ |a, A^{\perp}\rangle,\ |a, A^{\perp\!\!\perp}\rangle,\ |a^{\perp}, B\rangle,\ |a^{\perp}, B^{\perp}\rangle,\ |a^{\perp}, B^{\perp\!\!\perp}\rangle\Big\} \tag{B.3}$$

to rotate the a-basis of states that are MU to $\{|j_z\rangle\}$ into the basis $\{|j_x\rangle\}$ while the A-basis turns into $\{|J_x\rangle\}$, as before. This maps $\mathcal{B}_1$ to

$$\Big\{|0_x, J_x\rangle,\ |1_x, \hat{U}'J_x\rangle\Big\}\,, \tag{B.4}$$

where we have introduced a unitary $\hat{U}'$ which parameterises all orthonormal bases of $\mathbb{C}^3$ relative to the x-basis. The requirement that the states of the pair $\{\mathcal{I}_1; \mathcal{B}_1\}$ be MU now turns into the problem of identifying all pairs of orthonormal bases of $\mathbb{C}^3$, namely $\{|J_z\rangle;\ |\hat{U}J_z\rangle\}$ and $\{|J_x\rangle;\ |\hat{U}'J_x\rangle\}$, such that all states of one set are MU to those of the other, viz.

$$|\langle J_z|\hat{U}'J_x\rangle|^2 = |\langle \hat{U}J_z|J_x\rangle|^2 = |\langle \hat{U}J_z|\hat{U}'J_x\rangle|^2 = \frac{1}{3}\,, \tag{B.5}$$

while $|\langle J_z|J_x\rangle|^2 = 1/3$ holds by construction. It is easy to see that these conditions are satisfied if the bases in (at least) one pair coincide or all four are different, i.e. they use up a complete set of MU bases in $\mathbb{C}^3$. In Appendix C we present a proof, due to A. Sudbery, that these are the *only* solutions of the constraints (B.5). Thus, if $\mathcal{I}_1$ is the standard basis $\{|j_z, J_z\rangle\}$, then we obtain the MU product pair

$$\mathcal{P}_1 = \{|j_z, J_z\rangle;\ |0_x, J_x\rangle, |1_x, \hat{R}_{\xi,\eta}J_x\rangle\}\,, \tag{B.6}$$

with $\{|\hat{R}_{\xi,\eta}J_x\rangle\}$ defined in Eq. (3.15). However, if we use the complete set of MU bases in $\mathbb{C}^3$ we obtain the MU product pair

$$\mathcal{P}_2 = \{|0_z, J_z\rangle, |1_z, J_y\rangle;\ |0_x, J_x\rangle, |1_x, J_w\rangle\}\,. \tag{B.7}$$

• $\{\mathcal{I}_1; \mathcal{B}_3\}$: The second basis reads explicitly

$$\mathcal{B}_3 = \Big\{|a, A\rangle,\ |a^\perp, A\rangle,\ |b, A^\perp\rangle,\ |b^\perp, A^\perp\rangle,\ |c, A^{\perp\!\perp}\rangle,\ |c^\perp, A^{\perp\!\perp}\rangle\Big\}\,, \tag{B.8}$$

and suitable LETs map it to

$$\{|j_x, 0_x\rangle, |\hat{r}_\sigma j_x, 1_x\rangle, |\hat{r}_\tau j_x, 2_x\rangle\}\ , \tag{B.9}$$

which involve two rotations of the basis $\{|j_x\rangle\}$ about the z-axis, $\hat{r}_\sigma$ and $\hat{r}_\tau$. The operator $\hat{U}$ in $\mathcal{I}_1$ must be chosen such that $\{|\hat{U}J_z\rangle\}$ is MU to the x-basis. All such $U(3)$-rotations are given by the two-parameter family

$$\hat{S}_{\zeta,\chi} = |0_x\rangle\langle 0_x| + e^{i\zeta}|1_x\rangle\langle 1_x| + e^{i\chi}|2_x\rangle\langle 2_x|\,, \tag{B.10}$$

diagonal in the x-basis, and defined in analogy to $\hat{R}_{\xi,\eta}$ in Eq. (3.15). Altogether, we obtain a four-parameter family of MU product pairs,

$$\mathcal{P}_3 = \{|0_z, J_z\rangle, |1_z, \hat{S}_{\zeta,\chi}J_z\rangle;\ |j_x, 0_x\rangle, |\hat{r}_\sigma j_x, 1_x\rangle, |\hat{r}_\tau j_x, 2_x\rangle\}\,. \tag{B.11}$$

• $\{\mathcal{I}_3; \mathcal{B}_3\}$: No pair results when we combine the product basis $\mathcal{B}_3$ with $\mathcal{I}_3$. The standard transformations to simplify $\mathcal{B}_3$ lead to

$$\Big\{|j_x, 0_x\rangle,\ |\hat{r}_\sigma j_x, 1_x\rangle,\ |\hat{r}_\tau j_x, 2_x\rangle\Big\}\,, \tag{B.12}$$

since both the b-basis and the c-basis must be MU to the standard basis. The only basis MU to the three bases $\{|j_x\rangle\}$, $\{|\hat{r}_\sigma j_x\rangle\}$, and $\{|\hat{r}_\tau j_x\rangle\}$, is the standard basis $\{|j_z\rangle\}$, which is also true for the case $\{|\hat{r}_\sigma j_x\rangle\} = \{|\hat{r}_\tau j_x\rangle\}$. Consequently, this would force the operators $\hat{u}$ and $\hat{v}$ to be the identity, in contradiction to the assumption that the three bases of $\mathbb{C}^2$ present in $\mathcal{I}_3$ do not coincide.

Appendix C

Proof of Theorem C.0.1

Here we report a proof by A. Sudbery that the conditions of Eq. (B.5) in Appendix B are only satisfied if the bases in (at least) one pair coincide or all four bases are mutually unbiased. If $\mathcal{B}_1$ and $\mathcal{B}_2$ are orthonormal bases, we write $\mathcal{B}_1 \,\mu\, \mathcal{B}_2$ to mean "$\mathcal{B}_1$ and $\mathcal{B}_2$ are mutually unbiased".

Theorem C.0.1. *Suppose $\mathcal{B}_0, \mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$ are orthonormal bases of $\mathbb{C}^3$ satisfying*

$$\{\mathcal{B}_0, \mathcal{B}_1\} \;\mu\; \{\mathcal{B}_2, \mathcal{B}_3\}.$$

Then either $\mathcal{B}_0$ and $\mathcal{B}_1$ are equivalent bases or $\mathcal{B}_2$ and $\mathcal{B}_3$ are equivalent bases or all four bases are mutually unbiased.

Let $\mathcal{B}_0, \mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$ be represented by unitary matrices I, U, V, W, respectively, where we have chosen $\mathcal{B}_0$ to be the standard basis of $\mathbb{C}^3$. We regard the bases U, UP and UD, with P a permutation matrix and D a diagonal, as equivalent bases. Note that if two orthonormal bases in $\mathbb{C}^3$, represented by unitary matrices U and V, are mutually unbiased, then $U^\dagger V$ (where the dagger denotes hermitian conjugation) is a complex Hadamard matrix H. We can write any (3×3) Hadamard matrix as

$$H = DFD' \text{ or } DF^\dagger D' \tag{C.1}$$

where D and D' are diagonal and $F \equiv F_3$ is the Fourier matrix defined in Eq. (3.16).

The condition $\mathcal{B}_2 \,\mu\, \mathcal{B}_0$ implies the unitary V is a Hadamard matrix, and since $F^\dagger = FP$, the basis $\mathcal{B}_2$ is equivalent to a basis represented by $V = DF$. Similarly, $\mathcal{B}_3$ is equivalent to a basis represented by $W = D'F$ where D' is diagonal. Now

$$\mathcal{B}_2 \,\mu\, \mathcal{B}_1 \quad \Longrightarrow \quad V^\dagger U = KF^{(1)}L, \tag{C.2}$$

$$\mathcal{B}_3 \,\mu\, \mathcal{B}_1 \quad \Longrightarrow \quad W^\dagger U = K'F^{(2)}L' \tag{C.3}$$

where K, L, K' and L' are diagonal and $F^{(i)}$ is either F or $F^\dagger$ $(i = 1, 2)$. Hence

$$U = DFKF^{(1)}L = D'FK'F^{(2)}L'. \tag{C.4}$$

We will now examine the relationship between U and the diagonal matrices D, K, L in the two cases $U = DFKFL$ and $U = DFKF^\dagger L$, respectively. We can assume the leading entries of D and L to be $d_{11} = l_{11} = 1$ by absorbing two phase factors in the diagonal matrix K.

Lemma C.0.2. *Suppose $U = DFKFL$ where D, K, L are diagonal unitary matrices with $D = diag(1, \alpha, \beta)$. Then either $U = PE$ where P is a permutation matrix and E is diagonal, or the matrix elements of U are all non-zero and satisfy*

$$u_{12}u_{23}u_{31} = u_{13}u_{21}u_{32} = u_{11}u_{22}u_{33}, \tag{C.5}$$

and α and β are given by

$$\alpha^3 = \frac{u_{21}u_{22}u_{23}}{u_{11}u_{12}u_{13}}, \tag{C.6}$$

$$\beta = \alpha^2 \frac{u_{12}u_{31}}{u_{21}u_{22}}. \tag{C.7}$$

Let $K = \mathrm{diag}(\gamma, \delta, \epsilon)$ and $L = \mathrm{diag}(1, \zeta, \eta)$. Then

$$U = \begin{pmatrix} a & \zeta b & \eta c \\ \alpha b & \alpha\zeta c & \alpha\eta a \\ \beta c & \beta\zeta a & \beta\eta b \end{pmatrix} \tag{C.8}$$

where

$$\begin{aligned} a &= \tfrac{1}{3}(\gamma + \delta + \epsilon), \\ b &= \tfrac{1}{3}(\gamma + \omega\delta + \omega^2\epsilon), \\ c &= \tfrac{1}{3}(\gamma + \omega^2\delta + \omega\epsilon). \end{aligned} \tag{C.9}$$

Suppose one of a, b, c were zero, say $a = 0$. Then, since γ, δ, ϵ all have modulus 1, they must form an equilateral triangle in the complex plane, so either $\delta = \omega\gamma$ and $\epsilon = \omega^2\gamma$, when $b = 0$ and $c = \gamma$, or $\delta = \omega^2\gamma$ and $\epsilon = \omega\gamma$, when $b = \gamma$ and $c = 0$. In both cases U is of the form PE.

If none of a, b, c are zero, then all the matrix elements of U are non-zero and equations (C.5), (C.6) and (C.7) follow immediately from (C.8).

Exactly similar arguments prove

Lemma C.0.3. *Suppose $U = DFKF^\dagger L$ where D, K, L are as in Lemma C.0.2. Then either $U = PE$ where P is a permutation matrix and E is diagonal, or the matrix elements of U are all non-zero and satisfy*

$$u_{11}u_{23}u_{32} = u_{12}u_{21}u_{33} = u_{13}u_{22}u_{31}, \tag{C.10}$$

while α is given by (C.6) *and β by*

$$\beta = \alpha^2 \frac{u_{13}u_{31}}{u_{21}u_{23}}. \tag{C.11}$$

We now return to eq. (C.4) and consider the four possibilities for $(F^{(1)}, F^{(2)})$.

Case 1: $U = DFKFL = D'FK'FL'$.

Let $D = \mathrm{diag}(1, \alpha, \beta)$, $D' = \mathrm{diag}(1, \alpha', \beta')$. Then, by Lemma C.0.2, either U is of the form PE (when the bases $\mathcal{B}_0$ and $\mathcal{B}_1$ are equivalent), or

$$\alpha^3 = \alpha'^3 \qquad \text{and} \qquad \frac{\beta'}{\beta} = \left(\frac{\alpha'}{\alpha}\right)^2. \tag{C.12}$$

Hence $\alpha' = \alpha$ or $\omega\alpha$ or $\omega^2\alpha$, so

$$D' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \beta \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega\alpha & 0 \\ 0 & 0 & \omega^2\beta \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega^2\alpha & 0 \\ 0 & 0 & \omega\beta \end{pmatrix}. \tag{C.13}$$

This gives

$$V = DF = \begin{pmatrix} 1 & 1 & 1 \\ \alpha & \omega\alpha & \omega^2\alpha \\ \beta & \omega^2\beta & \omega\beta \end{pmatrix}, \tag{C.14}$$

$$W = D'F = \begin{pmatrix} 1 & 1 & 1 \\ \alpha & \omega\alpha & \omega^2\alpha \\ \beta & \omega^2\beta & \omega\beta \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 1 & 1 \\ \omega\alpha & \omega^2\alpha & \alpha \\ \omega^2\beta & \omega\beta & \beta \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 1 & 1 \\ \omega^2\alpha & \alpha & \omega\alpha \\ \omega\beta & \beta & \omega^2\beta \end{pmatrix}. \tag{C.15}$$

In each case the columns of W are a permutation of those of V. Thus either the bases $\mathcal{B}_0$ and $\mathcal{B}_1$ are equivalent or $\mathcal{B}_2$ and $\mathcal{B}_3$ are equivalent.

Case 2: $U = DFKFL = D'FK'F^\dagger L'$.

Suppose U is not of the form PE. Then both Lemmas C.0.2 and C.0.3 apply, and U has non-zero matrix elements satisfying (C.5) and (C.10). As in case 1, let $D = \text{diag}(1, \alpha, \beta)$ and $D' = \text{diag}(1, \alpha', \beta')$. Now α and β are given by Lemma C.0.2, but α' and β' are given by Lemma C.0.3. Once again we have $\alpha^3 = \alpha'^3$, but now β'/β is not determined solely by α'/α:

$$\frac{\beta'}{\beta} = \left(\frac{\alpha'}{\alpha}\right)^2 \frac{u_{13}u_{22}}{u_{12}u_{23}}. \tag{C.16}$$

Using (C.5) and (C.10),

$$\begin{aligned} \left(\frac{u_{13}u_{22}}{u_{12}u_{23}}\right)^3 &= \left(\frac{u_{13}}{u_{12}}\right)^3 \left(\frac{u_{22}}{u_{23}}\right)^3 \\ &= \frac{u_{13}}{u_{12}}.\frac{u_{23}u_{31}}{u_{21}u_{32}}.\frac{u_{21}u_{33}}{u_{22}u_{31}}.\frac{u_{22}}{u_{23}}.\frac{u_{12}u_{31}}{u_{11}u_{33}}.\frac{u_{11}u_{32}}{u_{13}u_{31}} \\ &= 1. \end{aligned} \tag{C.17}$$

Hence α'/α and β'/β are both cube roots of 1. Write $\alpha' = \phi\alpha$, $\beta' = \chi\beta$. If $\chi = \phi^2$ then, as shown in Case 1, the columns of V and W are the same, up to permutation, and the bases $\mathcal{B}_2$ and $\mathcal{B}_3$ are equivalent. If $\chi \neq \phi^2$ then two of $1, \chi, \phi$ are equal and the third is different. The same is true of the sets $\{1, \omega\chi, \omega^2\phi\}$ and $\{1, \omega^2\chi, \omega\phi\}$. Hence the sums $a = 1 + \chi + \phi$, $b = 1 + \omega\chi + \omega^2\phi$ and $c = 1 + \omega^2\chi + \omega\phi$ all have the same modulus. For $\chi \neq \phi^2$, the product

$$V^\dagger W = F^\dagger D^\dagger D' F = \frac{1}{3}\begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix}. \tag{C.18}$$

is a Hadamard matrix and hence the bases $\mathcal{B}_2$ and $\mathcal{B}_3$ are mutually unbiased. Thus in this case, $\mathcal{B}_2$ and $\mathcal{B}_3$ are either equivalent or mutually unbiased.

Case 3: $U = DFKF^\dagger L = D'FK'FL'$.

This is the same as Case 2 with V and W interchanged.

Case 4: $U = DFKF^\dagger L = D'FK'F^\dagger L'$.

This is similar to Case 1, using Lemma C.0.3 instead of Lemma C.0.2. The conclusion is the same.

We have now shown that in every case, either $\mathcal{B}_2$ and $\mathcal{B}_3$ are equivalent or $\mathcal{B}_0$ and $\mathcal{B}_1$ are equivalent or $\mathcal{B}_2$ and $\mathcal{B}_3$ are mutually unbiased. But the assumptions of the theorem are symmetric between the pairs $\{\mathcal{B}_0, \mathcal{B}_1\}$ and $\{\mathcal{B}_2, \mathcal{B}_3\}$, so we can also prove that if $\mathcal{B}_2$ is not equivalent to $\mathcal{B}_3$ and $\mathcal{B}_0$ is not equivalent to $\mathcal{B}_1$, then $\mathcal{B}_0$ and $\mathcal{B}_1$ are mutually unbiased and therefore all four bases are mutually unbiased.

Appendix D

Explicit construction of $BH(10,5)$ and $BH(14,7)$

In this Appendix we list the two Butson-type Hadamard matrices $BH(2p,p)$ of order 10 and 14 which we derive from the construction given in Butson's original paper [24].

• For $p=5$, the dephased matrix $BH(10,5)$ is given by

$$B_{10}=\frac{1}{\sqrt{10}}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^2 & \omega^4 & \omega & \omega^3 & 1 \\ 1 & \omega^2 & \omega^4 & \omega & \omega^3 & \omega^3 & \omega^2 & \omega & 1 & \omega^4 \\ 1 & \omega^3 & \omega & \omega^4 & \omega^2 & \omega^3 & \omega^4 & 1 & \omega & \omega^2 \\ 1 & \omega^4 & \omega^3 & \omega^2 & \omega & \omega^2 & 1 & \omega^3 & \omega & \omega^4 \\ 1 & \omega^3 & \omega^2 & \omega^2 & \omega^3 & 1 & \omega & \omega^4 & \omega^4 & \omega \\ 1 & \omega^2 & 1 & \omega^4 & \omega^4 & \omega & \omega & \omega^3 & \omega^2 & \omega^3 \\ 1 & \omega & \omega^3 & \omega & 1 & \omega^4 & \omega^3 & \omega^4 & \omega^2 & \omega^2 \\ 1 & 1 & \omega & \omega^3 & \omega & \omega^4 & \omega^2 & \omega^2 & \omega^4 & \omega^3 \\ 1 & \omega^4 & \omega^4 & 1 & \omega^2 & \omega & \omega^3 & \omega^2 & \omega^3 & \omega \end{pmatrix}, \qquad \text{(D.1)}$$

where $\omega = e^{2\pi i/5}$ is a fifth root of unity. The defect of B_{10} is zero.

• For $p=7$, the dephased matrix $BH(14,7)$ is

$$B_{14} = \frac{1}{\sqrt{14}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^6 & \omega^2 & \omega^5 & \omega & \omega^4 & 1 & \omega^3 \\ 1 & \omega^2 & \omega^4 & \omega^6 & \omega & \omega^3 & \omega^5 & \omega^3 & \omega^2 & \omega & 1 & \omega^6 & \omega^5 & \omega^4 \\ 1 & \omega^3 & \omega^6 & \omega^2 & \omega^5 & \omega & \omega^4 & \omega^5 & 1 & \omega^2 & \omega^4 & \omega^6 & \omega & \omega^3 \\ 1 & \omega^4 & \omega & \omega^5 & \omega^2 & \omega^6 & \omega^3 & \omega^5 & \omega^3 & \omega & \omega^6 & \omega^4 & \omega^2 & 1 \\ 1 & \omega^5 & \omega^3 & \omega & \omega^6 & \omega^4 & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & 1 & \omega & \omega^2 \\ 1 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega & \omega^6 & \omega^3 & 1 & \omega^4 & \omega & \omega^5 & \omega^2 \\ 1 & \omega^4 & \omega^2 & \omega & \omega & \omega^2 & \omega^4 & 1 & \omega^5 & \omega^6 & \omega^3 & \omega^3 & \omega^6 & \omega^5 \\ 1 & \omega & \omega^3 & \omega^6 & \omega^3 & \omega & 1 & \omega^4 & \omega^6 & \omega^4 & \omega^5 & \omega^2 & \omega^2 & \omega^5 \\ 1 & \omega^5 & \omega^4 & \omega^4 & \omega^5 & 1 & \omega^3 & \omega^2 & \omega & \omega^3 & \omega & \omega^2 & \omega^6 & \omega^6 \\ 1 & \omega^2 & \omega^5 & \omega^2 & 1 & \omega^6 & \omega^6 & \omega & \omega^4 & \omega^3 & \omega^5 & \omega^3 & \omega^4 & \omega \\ 1 & \omega^6 & \omega^6 & 1 & \omega^2 & \omega^5 & \omega^2 & \omega & \omega & \omega^4 & \omega^3 & \omega^5 & \omega^3 & \omega^4 \\ 1 & \omega^3 & 1 & \omega^5 & \omega^4 & \omega^4 & \omega^5 & \omega^2 & \omega^6 & \omega^6 & \omega^2 & \omega & \omega^3 & \omega \\ 1 & 1 & \omega & \omega^3 & \omega^6 & \omega^3 & \omega & \omega^4 & \omega^5 & \omega^2 & \omega^2 & \omega^5 & \omega^4 & \omega^6 \end{pmatrix}, \tag{D.2}$$

with $\omega = e^{2\pi i/7}$ a seventh root of unity. This matrix has zero defect.

Bibliography

[1] Matlab version 7.14 (r2012a), the mathworks inc.

[2] S. S. Agaian. Hadamard matrices and applications. *Springer Lecture Notes in Mathematics, Springer-Verlag, Berlin*, 1985.

[3] P. K. Aravind. Solution to the king's problem in prime power dimensions. *Zeitschrift für Naturforschung. A*, 58(2-3):85–92, 2003.

[4] C. Archer. There is no generalization of known formulas for mutually unbiased bases. *Journal of mathematical physics*, 46:022106, 2005.

[5] M. Aschbacher, A. M. Childs, and P. Wocjan. The limitations of nice mutually unbiased bases. *J. Algebraic Combin.*, 25(2):111–123, 2007.

[6] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan. A new proof for the existence of mutually unbiased bases. *Algorithmica*, 34(4):512–528, 2002.

[7] T. Banica and R. Nicoara. Quantum groups and Hadamard matrices. *Panamer. Math. J.*, 17(1):1–24, 2007.

[8] N. Barros e Sá and I. Bengtsson. Families of complex Hadamard matrices. *Arxiv preprint arXiv:1202.1181*, 2012.

[9] K. Beauchamp and R. Nicoara. Orthogonal maximal abelian *-subalgebras of the 6×6 matrices. *Lin. Alg. Appl.*, 428(8-9):1833–1853, 2008.

[10] I. Bengtsson, W. Bruzda, Å. Ericsson, J-Å. Larsson, W. Tadej, and K. Życzkowski. Mutually unbiased bases and Hadamard matrices of order six. *J. Math. Phys.*, 48(5):052106, 21, 2007.

[11] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175. Bangalore, India, 1984.

[12] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters. Quantum nonlocality without entanglement. *Physical Review A*, 59(2):1070, 1999.

[13] G. Björck and R. Fröberg. A faster way to count the solutions of inhomogeneous system of algebraic equations, with applications to cyclic n-roots. *J. Symbolic Comput.*, 12(3):329–336, 1991.

[14] G. Björck and B. Saffari. New classes of finite unimodular sequences with unimodular fourier transforms. Circulant Hadamard matrices with complex entries. *CR Acad. Sci. Paris Sér. I Math.*, 320(3):319–324, 1995.

[15] P. O. Boykin and V. P. Roychowdhury. Information vs. disturbance in dimension D. *Quantum Inf. Comput.*, 5(4-5):396–412, 2005.

[16] S. Brierley and S. Weigert. Maximal sets of mutually unbiased quantum states in dimension 6. *Phys. Rev. A*, 78(4):042312, 8, 2008.

[17] S. Brierley and S. Weigert. Constructing mutually unbiased bases in dimension six. *Phys. Rev. A*, 79(5):052316, 13, 2009.

[18] S. Brierley and S. Weigert. Mutually unbiased bases and semi-definite programming. *J. Phys.: Conference Series*, 254:012008, 2010.

[19] S. Brierley, S. Weigert, and I. Bengtsson. All mutually unbiased bases in dimensions two to five. *Quantum Information & Computation*, 10(9):803–820, 2010.

[20] R. H. Bruck and H. J. Ryser. The nonexistence of certain finite projective planes. *Canad. J. Math*, 1(191):9, 1949.

[21] W. Bruzda, W. Tadej, and K. Życzkowski. A catalogue of complex Hadamard matrices. `http://chaos.if.uj.edu.pl/∼karol/hadamard`.

[22] J. Bub. *Interpreting the quantum world.* Cambridge University Press, 1999.

[23] P. Busch and P. J. Lahti. The complementarity of quantum observables: theory and experiments. *La Rivista del Nuovo Cimento (1978-1999)*, 18(4):1–27, 1995.

[24] A. T. Butson. Generalized Hadamard matrices. In *Proc. Amer. Math. Soc*, volume 13, pages 894–898, 1962.

[25] P. Butterley and W. Hall. Numerical evidence for the maximum number of mutually unbiased bases in dimension six. *Phys. Lett. A*, 369(1-2):5–8, 2007.

[26] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin. Security of quantum key distribution using d-level systems. *Phys. Rev. Lett.*, 88(12):127902, 2002.

[27] B. Compton, R. Craigen, and W. de Launey. Unreal BH(n,6)'s and Hadamard matrices. *preprint*, 2008.

[28] P. Diţă. Some results on the parametrization of complex Hadamard matrices. *J. Phys. A: Math. Gen.*, 37:5355, 2004.

[29] P. Diţă. Complex Hadamard matrices from Sylvester inverse orthogonal matrices. *Open Syst. & Inf. Dyn.*, 16(4):387–405, 2009.

[30] P. Diţă. Hadamard matrices from mutually unbiased bases. *J. Math. Phys.*, 51:072202, 2010.

[31] T. Durt. About mutually unbiased bases in even and odd prime power dimensions. *J. Phys. A*, 38(23):5267–5283, 2005.

[32] B. -G. Englert and Y. Aharonov. The mean king's problem: prime degrees of freedom. *Phys. Lett. A*, 284(1):1–5, 2001.

[33] C. Godsil and A. Roy. Equiangular lines, mutually unbiased bases, and spin models. *European Journal of Combinatorics*, 30(1):246–262, 2009.

[34] M. Grassl. On SIC-POVMs and MUBs in dimension 6. *Proc. ERATO Conf. on Quantum Information Science 2004 (EQIS 2004); e-print arXiv:quant-ph/0406175*, 2004.

[35] U. Haagerup. Orthogonal maximal abelian *-subalgebras of the $n \times n$ matrices and cyclic n-roots. In *Operator algebras and quantum field theory (Rome, 1996)*, pages 296–322. Int. Press, Cambridge, MA, 1997.

[36] J. Hadamard. Résolution d'une question relative aux déterminants. *Bull. Sci. Math*, 17(1):240–246, 1893.

[37] A. Hayashi, M. Horibe, and T. Hashimoto. Mean king's problem with mutually unbiased bases and orthogonal Latin squares. *Phys. Rev. A (3)*, 71(5):052331, 4, 2005.

[38] T. Heinosaari and M. Ziman. *The mathematical language of quantum theory: from uncertainty to entanglement.* Cambridge University Press, 2011.

[39] K. J. Horadam. *Hadamard matrices and their applications.* Princeton, NJ: Princeton University Press, 2007.

[40] R. Hosoya and H. Suzuki. Type II matrices and their Bose-Mesner algebras. *J. Algebraic Combinatorics*, 17(1):19–37, 2003.

[41] R. Howe. Nice error bases, mutually unbiased bases, induced representations, the Heisenberg group and finite geometries. *Indagationes Mathematicae*, 16(3):553–583, 2005.

[42] C. J. Isham. *Lectures on quantum theory: mathematical and structural foundations.* Allied Publishers, 2001.

[43] I. D. Ivanović. Geometrical description of quantal state determination. *J. Phys. A: Math. Gen.*, 14(12):3241–3245, 1981.

[44] P. Jaming, M. Matolcsi, and P. Móra. The problem of mutually unbiased bases in dimension 6. *Cryptography and Communications*, 2(2):211–220, 2010.

[45] P. Jaming, M. Matolcsi, P. Móra, F. Szöllősi, and M. Weiner. A generalized Pauli problem and an infinite family of MUB-triplets in dimension 6. *J. Phys. A*, 42(24):245305, 25, 2009.

[46] W. M. Kantor. MUBs inequivalence and affine planes. *Journal of Mathematical Physics*, 53:032204, 2012.

[47] B. R. Karlsson. Two-parameter complex Hadamard matrices for $N = 6$. *J. Math. Phys.*, 50(8):082104, 8, 2009.

[48] B. R. Karlsson. H2-reducible complex hadamard matrices of order 6. *Linear Algebra and its Applications*, 434(1):239–246, 2011.

[49] B. R. Karlsson. Three-parameter complex Hadamard matrices of order 6. *Lin. Alg. Appl.*, 434(1):247–258, 2011.

[50] G. Kimura, H. Tanaka, and M. Ozawa. Solution to the mean king's problem with mutually unbiased bases for arbitrary levels. *Physical Review A*, 73(5):050301, 2006.

[51] A. Klappenecker and M. Rötteler. Constructions of mutually unbiased bases. In *Finite fields and applications*, volume 2948 of *Lecture Notes in Comput. Sci.*, pages 137–144. Springer, Berlin, 2004.

[52] A. Klappenecker and M. Rötteler. Mutually unbiased bases are complex projective 2-designs. In *Information Theory, 2005. ISIT 2005. Proceedings. International Symposium on*, pages 1740–1744. IEEE, 2005.

[53] A. Klappenecker and M. Rötteler. On the monomiality of nice error bases. *IEEE Trans. Inform. Theory*, 51(3):1084–1089, 2005.

[54] A. B. Klimov, J. L. Romero, G. Björk, and L. L. Sánchez-Soto. Geometrical approach to mutually unbiased bases. *J. Phys. A*, 40(14):3987–3998, 2007.

[55] A. I. Kostrikin and P. H. Tiep. *Orthogonal decompositions and integral lattices*, volume 15. de Gruyter, 1994.

[56] C. W. H. Lam, L. Thiel, and S. Swiercz. The non-existence of finite projective planes of order 10. *Canad. J. Math*, 41(6):1117–1123, 1989.

[57] P. H. J. Lampio, F. Szöllősi, and P. R. J Östergård. The quaternary complex Hadamard matrices of orders 10, 12, and 14. *Discrete Mathematics*, 313(2):189 – 206, 2013.

[58] J. Lawrence. Entanglement patterns in mutually unbiased basis sets. *Phys. Rev. A*, 84(2):022338, 2011.

[59] G. W. Mackey. *Mathematical foundations of quantum mechanics.* Dover Publications, 2004.

[60] M. Matolcsi. A Fourier analytic approach to the problem of mutually unbiased bases. *Studia Scientiarum Mathematicarum Hungarica*, 49(4):482–491, 2012.

[61] M. Matolcsi, J. Réffy, and F. Szöllosi. Constructions of complex Hadamard matrices via tiling abelian groups. *Open Syst. & Inf. Dyn.*, 14(3):247–263, 2007.

[62] M. Matolcsi, I. Z. Ruzsa, and M. Weiner. Real and complex unbiased Hadamard matrices. *Arxiv preprint arxiv:1201.0631*, 2012.

[63] M. Matolcsi and F. Szöllősi. Towards a classification of 6 × 6 complex hadamard matrices. *Open Systems & Information Dynamics*, 15(02):93–108, 2008.

[64] G. McConnell and D. Gross. Efficient 2-designs from bases exist. *Quantum Inf. Comput.*, 8(8-9):734–740, 2008.

[65] G. E. Moorhouse. The 2-transitive complex Hadamard matrices. *preprint available at http://www.uwyo.edu/moorhouse/pub*, 2001.

[66] R. Nicoara. A finiteness result for commuting squares of matrix algebras. *J. Operator Theory*, 55(2):295–310, 2006.

[67] M. A. Nielsen. Conditions for a class of entanglement transformations. *Phys. Rev. Lett.*, 83(2):436–439, 1999.

[68] T. Paterek, B. Dakić, and Č. Brukner. Mutually unbiased bases, orthogonal Latin squares, and hidden-variable models. *Phys. Rev. A (3)*, 79(1):012109, 6, 2009.

[69] M. K. Patra. Quantum state determination: estimates for information gain and some exact calculations. *J. Phys. A*, 40(35):10887–10902, 2007.

[70] M. Petrescu. *Existence of continuous families of complex Hadamard matrices of certain prime dimensions and related results.* PhD thesis, University of California, Los Angeles, 1997.

[71] D. Petz. Complementarity in quantum systems. *Reports on Mathematical Physics*, 59(2):209–224, 2007.

[72] M. Planat, H. C. Rosu, and S. Perrine. A survey of finite algebraic geometrical structures underlying mutually unbiased quantum measurements. *Foundations of Physics*, 36(11):1662–1680, 2006.

[73] S. Popa. Orthogonal pairs of *-subalgebras in finite von Neumann algebras. *J. Operator Theory*, 9(2):253–268, 1983.

[74] P. Raynal, X. Lü, and B. -G. Englert. Mutually unbiased bases in six dimensions: The four most distant bases. *Physical Review A*, 83(6):062303, 2011.

[75] J. L. Romero, G. Björk, A. B. Klimov, and L. L. Sánchez-Soto. Structure of the sets of mutually unbiased bases for N qubits. *Phys. Rev. A*, 72(6):062310, 2005.

[76] A. Roy and A. J. Scott. Weighted complex projective 2-designs from bases: optimal state determination by orthogonal measurements. *Journal of mathematical physics*, 48(7):072110–072110, 2007.

[77] M. Saniga and M. Planat. Viewing sets of mutually unbiased bases as arcs in finite projective planes. *Chaos Solitons Fractals*, 26(5):1267–1270, 2005.

[78] M. Saniga, M. Planat, and H. Rosu. Mutually unbiased bases and finite projective planes. *J. Opt. B Quantum Semiclass. Opt.*, 6(9):L19–L20, 2004.

[79] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3):1301, 2009.

[80] J. Schwinger. Unitary operator bases. *Proc. Nat. Acad. Sci. U.S.A.*, 46:570–579, 1960.

[81] A. J. Scott. Tight informationally complete quantum measurements. *J. Phys. A*, 39(43):13507–13530, 2006.

[82] A. J. Skinner, V. A. Newell, and R. Sanchez. Unbiased bases (Hadamards) for six-level systems: four ways from Fourier. *J. Math. Phys.*, 50(1):012107, 7, 2009.

[83] J. J. Sylvester. Thoughts on inverse orthogonal matrices, simultaneous signsuccessions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers. *Phil. Mag.*, 34(232):461–475, 1867.

[84] F. Szöllősi. Parametrizing complex Hadamard matrices. *Eur. J. Combin.*, 29(5):1219–1234, 2008.

[85] F. Szöllősi. A two-parameter family of complex Hadamard matrices of order 6 induced by hypocycloids. *Proc. Amer. Math. Soc.*, 138(3):921–928, 2010.

[86] F. Szöllősi. Construction, classification and parametrization of complex Hadamard matrices. *PhD thesis, Central European University, Arxiv preprint arXiv:1110.5590*, 2011.

[87] F. Szöllősi. Complex Hadamard matrices of order 6: a four-parameter family. *Journal of the London Mathematical Society*, 85(3):616–632, 2012.

[88] W. Tadej and K. Życzkowski. A concise guide to complex Hadamard matrices. *Open Syst. Inf. Dyn.*, 13(2):133–177, 2006.

[89] T. Tao. Fuglede's conjecture is false in 5 and higher dimensions. *Math. Res. Lett.*, 11(2-3):251–258, 2004.

[90] L. Vaidman, Y. Aharonov, and D. Z. Albert. How to ascertain the values of σ_x, σ_y, and σ_z of a spin-$\frac{1}{2}$ particle. *Phys. Rev. Lett.*, 58(14):1385–1387, 1987.

[91] S. Weigert and T. Durt. Affine constellations without mutually unbiased counterparts. *J. Phys. A*, 43(40):402002, 6, 2010.

[92] R. F. Werner. All teleportation and dense coding schemes. *J. Phys. A: Math. Gen.*, 34:7081, 2001.

[93] M. Wieśniak, T. Paterek, and A. Zeilinger. Entanglement in mutually unbiased bases. *New Journal of Physics*, 13(5):053047, 2011.

[94] E. Wigner. *Gruppentheorie und ihre Anwendung auf die Quantenmechanik der Atomspektren.* J. W. Edwards, Ann Arbor, Michigan, 1944.

[95] P. Wocjan and T. Beth. New construction of mutually unbiased bases in square dimensions. *Quantum Inf. Comput.*, 5(2):93–101, 2005.

[96] W. K. Wootters. Quantum measurements and finite geometry. *Found. Phys.*, 36(1):112–126, 2006.

[97] W. K. Wootters and B. D. Fields. Optimal state-determination by mutually unbiased measurements. *Ann. Phys.*, 191(2):363–381, 1989.

[98] G. Zauner. Quantum designs: Foundations of a noncommutative design theory. *Int. J. Quantum Inf.*, 9(1):445–507, 2011.